

القوة الإلكترونية

كيف يمكن أن تُدير الدول شؤونها في عصر الإنترنت

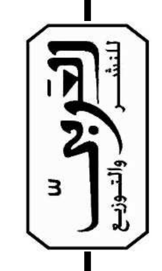
إيهاب خليفة

العربي للنشر والتوزيع

القوة الإلكترونية.. كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت؟
"الولايات المتحده نموذجاً"
إيهاب خليفة

الطبعةالأولى: 2017

رقم الإيداع: 2017/1766
الترقيم الدولي: 978977319 3232
الغلاف: الاء هيكل



60 شارع القصر العيني - 11451 - القاهرة
ت 27921943 - 27954529 فاكس 27947566
Www.Alarabipublishing.Com.Eg

بطاقة فهرسة
خليفة، إيهاب
القوى الإلكترونية.. كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت؟/إيهاب خليفة ،
القاهرة: العربي للنشر والتوزيع، 2017- ص؛ سم.
تدمك: 9789773193 3232
1- العلاقات الخارجيه – تطبيقات الحاسب
2- الاحوال الاقتصاديه – تطبيقات الحاسب
3- الولايات المتحده الامريكيه – علاقات خارجيه
أ- العنوان 327.285

القوة الإلكترونية

كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت؟

"الولايات المتحدة الأمريكية نموذجاً"

إيهاب خليفة



تقديم:

إذا كان الفحم هو محرك الثورة الصناعية التي شهدها العالم في القرن الثامن عشر، **فإن الإنترنت هي محرك الثورة التكنولوجية التي شهدها العالم في بدايات القرن الحادي والعشرين**، وإذا جاز أن نطلق تسمية على هذا العصر الذي نعيش فيه، فهو عصر "الإنترنت" بامتياز، حيث ساهمت الانترنت في تغير أشكال وأنماط الحياة، بل والحكومات والدول، وغيرت من المفاهيم التقليدية للقوة، فظهرت الحكومات الإلكترونية، ثم تطورت إلى الحكومات الذكية، ومنها إلى المدن الذكية، وليس من الغريب أن نجد قريباً دولة بأكملها أصبحت ذكية، تعتمد على الإنترنت وأجهزة التليفون المحمول في الحصول على الخدمات كافة وإنهاء المعاملات كافة.

وقد كان لظهور الفضاء الإلكتروني والشبكة العنكبوتية أثر مهم في الحياة البشرية، فسهولة استخدامها ورخص تكلفتها ساعد على قيامها بأدوار مختلفة في الحياة البشرية، سواء تجارية أو اقتصادية أو معلوماتية أو سياسية أو عسكرية أو أيديولوجية أو غيرها، ومن هنا ظهر مفهوم جديد يمكن أن نطلق عليه **مفهوم "القوة الإلكترونية**[1]. "Cyber Power" فالذي يدير العالم الآن آحاد وأصفار غاية في الصغر، وقد أصبح جلياً أن من يمتلك آليات توظيف هذه البيئة الإلكترونية الجديدة فإنه الأكثر قدرة على التأثير في سلوك الفاعلين المستخدمين لهذه البيئة.

وكما ساعدت الإنترنت في تحقيق رفاهية الحياة الإنسانية، أصبحت أيضاً مصدراً لتهديدها، حيث يستطيع أحد مستخدمي الفضاء الإلكتروني أن يوقع خسائر فادحة بالطرف الآخر، وأن يتسبب في شل البينة المعلوماتية والاتصالاتية الخاصة به، وهو ما يسبب خسائر عسكرية واقتصادية فادحة، من خلال قطع أنظمة الاتصال بين الوحدات العسكرية وبعضها البعض أو تضليل معلوماتها أو سرقة معلومات سرية عنها، أو من خلال التلاعب بالبيانات الاقتصادية والمالية وتزييفها أو مسحها من أجهزة الحواسب، **وعلى الرغم من فداحة الخسائر فإن الأسلحة بسيطة لا**

1- لعله من الضروري الإشارة إلى أن مصطلح "القوة الإلكترونية" غير دقيق علمياً، والأصح هو مصطلح **"القوة السيبرية"**، لأنه الترجمة الحرفية للمصطلح الإنجليزية "Cyber Power "، مثلما أن "الإلكترونية" هي الترجمة الحرفية لكلمة "Electronic"، ولكن نظراً لعدم شيوع استخدام كلمة "السيبرية" في الأدبيات العربية، تم اعتماد مصطلح "القوة الإلكترونية" باعتباره الأكثر شيوعاً، وذلك بهدف التسهيل على القارئ.

تتعدى الكيلوبايتس، تمثل في فيروسات إلكترونية تخترق شبكة الحاسب الآلي وتنتشر بسرعة بين الأجهزة، وتبدأ عملها في سرية تامة وبكفاءة عالية، وهي في ذلك لا تفرق بين المقاتل والمدني وبين العام والخاص وبين السري والمعلوم.

ومن هنا جاءت فكرة إعداد هذا الكتاب، الذي هو في الأصل رسالة ماجستير تم تقديمها بكلية الاقتصاد والعلوم السياسية جامعة القاهرة، بهدف معرفة التغيرات التي طرأت على مفاهيم القوة وممارسة النفوذ في العلاقات الدولية بفضل الإنترنت، وكيف أصبحت مصدر تهديد للدول والأفراد، ومعرفة المخاطر التي يمكن أن يتعرض لها الأمن القومي للدول عبر الإنترنت، مع دراسة النموذج الأمريكي في توظيفه للقوة الإلكترونية، وكيف أصبحت مصدر نفوذ أو تهديد للأمن القومي الأمريكي؟

وقد تم إعداد هذا الكتاب من ثلاثة فصول رئيسية، يناقش الفصل الأول التغيرات التي طرأت على مفهوم القوة بفضل الإنترنت، وكيف ظهرت القوة الإلكترونية، ويتطرق الفصل الثاني إلى عناصر القوة الإلكترونية الأمريكية، من حيث المصالح والتهديدات في الفضاء الإلكتروني، والاستراتيجيات المتبعة للتعامل معها، ويتناول الفصل الثالث تطبيقات لاستخدام القوة الإلكترونية - خاصة الأمريكية – سواء كانت سياسية أو اقتصادية أو عسكرية بهدف تحقيق التفوق وممارسة النفوذ في العلاقات الدولية.

وفي النهاية لا يسعني إلا أن أشكر كل من ساهم في إخراج هذا العمل، سواء كان من أساتذتي بكلية الاقتصاد والعلوم السياسية، خاصة الأستاذة الدكتورة نازلي معوض والأستاذة الدكتورة سعاد محمود، اللتين أشرفتا على إعداد رسالة الماجستير التي اعتمد عليها هذا الكتاب، وأن أهدي ثمرة جهدي المتواضعة هذه إلى روح أبي الطاهرة الذي طالما تمنيت أن يكون معي مرشداً ومعلماً، وإلى أمي التي كانت مصدر الحماس الدائم بالنسبة لي، وإلى زوجتي التي وقفت بجانبي حتى إخراج هذا العمل، وإلى إخوتي مؤمن ومحمد وإلى اصدقائي وكل من شجعني ولو بكلمة حتى إتمام هذا الكتاب.

إيهاب خليفة

أبوظبي، 1 يناير 2017

المقدمة:

عرفت الإنسانية في صراعها نحو البقاء بيئات طبيعية سعت لاستكشافها واستغلالها وفرض نفوذها عليها بداية من الأرض أو الإقليم البري، الذي استطاع الإنسان أن يفرض عليه سيطرته في المناطق التي سمحت له الطبيعة بذلك وساعدته على تحقيق ذلك، ومع الرغبة في اكتشاف المناطق البعيدة من العالم قام الإنسان باستكشاف بيئة أخرى وهي البحر أو الإقليم البحري، مستخدماً في ذلك أخشاب الأشجار، ومع تطور التكنولوجيا من استخدام الدواب إلى السيارات والقطارات والطائرات ومن المراكب الشراعية إلى السفن البخارية والغواصات النووية، أصبح للتكنولوجيا دور مهم في اكتشاف الطبيعة، وبدأ الانسان يفرض سيطرته عليها تدريجياً.

ومع ظهور النعرات الطائفية والوطنية، مع دافع من الرغبة في البقاء على قيد الحياة وتحقيق النفوذ، بدأ تطويع التكنولوجيا لتخدم أهدافه التوسعية ... وحسم المعارك الحربية، فظهرت أهمية القوة البحرية إلى جانب القوة البرية، ومع التطور التكنولوجي أمكن القفز لبيئة طبيعية أخرى، وهي **الجو أو الإقليم الجوي**، وبدأت تحلق فيه الطائرات وظهرت أهميتها في تدمير مواقع العدو والتمهيد للمعارك الحربية، ومع التطور التكنولوجي المذهل في عالم الطيران والصواريخ أمكن استغلال بيئة طبيعية جديدة، وهي **الفضاء الخارجي**، من خلال الصواريخ والأقمار الصناعية، وعلى الرغم من أن الفضاء الخارجي لم يتم استغلاله عسكرياً أو تجارياً مثلما تم استغلال البيئات الثلاث السابقة، فإنه يشكل محوراً مهماً في ربط البيئات الطبيعية الأخرى بعضها البعض، حيث تتزايد أهميته في عالم الاتصالات والمعلومات.

وبفضل ثورة المعلومات، ومع ظهور الإنترنت ومواقع الويب ظهرت لدينا بيئة أخرى وهي **الفضاء الإلكتروني**، وعلى الرغم من أنها تختلف عن البيئات الأربع الطبيعية السابقة في كونها بيئة من صنع الإنسان ManMade، فإنها تتمتع بخصائص تشترك فيها مع تلك البيئات السابقة، وأصبح الفضاء الإلكتروني أحد العناصر الرئيسية التي تؤثر في النظام الدولي بما يحمل من أدوات تكنولوجية تلعب دوراً مهماً في عملية التعبئة والحشد في العالم، فضلاً عن التأثير في القيم السياسية،

فسهولة استخدامها ورخص تكلفتها ساعدا على قيامها بأدوار مختلفة في الحياة البشرية، سواء تجارية أو اقتصادية أو معلوماتية أو سياسية أو عسكرية أو أيديولوجية، هذا فضلاً على أنها لم تعُد حكراً على الدول فقط، بل إن شركات التكنولوجيا العملاقة هي التي تسيطر بدرجة ما على المقومات التكنولوجيا، وقد أصبح جلياً أن من يمتلك آليات توظيف هذه البيئة الإلكترونية الجديدة يصبح الأكثر قدرة على تحقيق أهدافه والتأثير في سلوك الفاعلين المستخدمين لهذه البيئة.

وقد استطاعت بعض الدول توظيف التكنولوجيا الحديثة في تعظيم قوتها، وظهر لدينا نوع جديد من القوة هو القوة الإلكترونية Cyber Power، والتي يقصد بها توظيف وسائل الاتصالات وتكنولوجيا المعلومات وشبكات الكمبيوتر والبرمجيات لتحقيق أهداف الدولة السياسية والاقتصادية والعسكرية والاجتماعية والثقافية وغيرها من الأهداف، حيث سعت الدول إلى الاستفادة من تلك القوة في تطوير استراتيجياتها العسكرية والسياسية من أجل حماية مصالحها الوطنية[1]، فالدولة عادةً ما تترجم قدراتها على تحقيق أهدافها الخارجية من خلال استخدامها وسائل مختلفة أهمها: الدبلوماسية، والقوة العسكرية، والدعاية، والأدوات الاقتصادية. ولكن أصبح من الأمور المستقرة في العلاقات الدولية أن مصادر قوة الدولة وأشكالها تتغير، فإلى جانب القوة الصلبة والتي تتمثل في القدرات العسكرية والاقتصادية، تزايد الاهتمام بالأبعاد غير المادية للقوة، ومن ثم برز دور القوة الناعمة التي تعتمد على جاذبية النموذج والإقناع، ومع ثورة المعلومات والقدرة على إنتاج التكنولوجيا المتطورة عن طريق الاختراع والإبداع، ظهر لدينا شكل جديد من أشكال القوة هو القوة الإلكترونية، وأصبح لديها تأثير على المستويين الدولي والمحلي، فمن ناحية أدت إلى توزيع وانتشار القوة بين عدد أكبر من الفاعلين مما جعل قدرة الدولة على السيطرة على هذا الميدان موضع شك، مقارنة بالمجالات الأخرى للقوة، ومن ناحية أخرى جعلت القوة الإلكترونية بعض الفاعلين الأصغر في السياسة الدولية لديهم

1- Richard L. Kugler, "From Cyber Space To Cyber Power: Defining The Problems", In Franklin D. Krammer, Stuart Starr, And Larry K. Wentz. Eds, **Cyber Power And National Security,** (Washington, D.C: National Defense Up, 2009), P316.

قدرة أكبر على ممارسة كل من القوة الصلبة والقوة الناعمة عبر الفضاء الإلكتروني Cyber Space، وهو ما يعني تغيراً في علاقات القوى في السياسة الدولية[1].

في إطار هذا السياق السابق، تتمثل القضية الرئيسية محل الدراسة في **رصد وتحليل كيفية استخدام الدولة للقوة الإلكترونية في إدارة تفاعلاتها الدولية،** وذلك بالتطبيق على الولايات المتحدة الأمريكية، في الفترة من 2001 حتى 2012؟

وللإجابة عن هذا السؤال، تتطرق الدراسة إلى عدد من الأسئلة الرئيسية من قبيل:

ما هو أثر ثورة المعلومات على انتشار القوة في السياسة الدولية؟ وكيف أثرت ثورة المعلومات على أبعاد التحول في مفهوم القوة؟ وما هي عناصر القوة الإلكترونية؟ ومن هم الفاعلون الرئيسيون في مجال استخدامها؟ وما هي طبيعة العلاقة بينها وبين الأشكال الأخرى للقوة؟ وكيف توظف القوة الإلكترونية في إدارة التفاعلات الدولية؟ وما هي القيود التي تحد من فاعلية استخدامها؟ وما هي مصالح الولايات المتحدة في عالم الفضاء الإلكتروني؟ وما هي مصادر التهديد لتلك المصالح؟ وما هي عناصر القوة الإلكترونية الأمريكية؟ وهل تغيرت العقيدة الأمريكية حول استخدام القوة الإلكترونية الأمريكية بتغير الرئاسة الأمريكية؟ وما هي أبعاد الاستراتيجية الأمريكية الحاكمة لاستخدام القوة الإلكترونية الأمريكية؟ وكيف وظفت الولايات المتحدة القوة الإلكترونية في إدارة تفاعلاتها الدولية جنباً إلى جنب الأشكال الأخرى للقوة؟ وإلى أي مدى نجحت في ذلك؟ وما هي القيود الواردة على هذا الاستخدام؟

1- د. سعاد محمود أبو ليلة، "دورة القوة: ديناميكيات الانتقال من "الصلبة" إلى " الناعمة" إلى "الافتراضية"، **مجلة السياسة الدولية، ملحق اتجاهات نظرية: القوة: كيف يمكن فهم تحولات القوة في السياسة الدولية؟**، العدد 188 (أبريل، 2012)، ص 16.

ويتناول الكاتب بالدراسة استخدام القوة الإلكترونية في إدارة التفاعلات الدولية مع التطبيق على الولايات المتحدة في الفترة من 2001 حتى عام 2012 وذلك للأسباب الآتية:

أ- شهدت بداية تلك الفترة هجمات الحادي عشر من سبتمبر 2001 على الولايات المتحدة، وما تلاها من إعلان الحرب على الإرهاب، وإضفاء مزيد من القوة على فاعلين من غير الدول كالجماعات الإرهابية[1].

ب- تعرضت الولايات المتحدة مع بداية فترة الدراسة للعديد من الهجمات الإلكترونية Cyber Attacks عالية المستوى[2]، ساهمت في إعلاء الاهتمام الأمريكي بالقوة الإلكترونية كوسيلة أساسية لإدارة التفاعلات الدولية بجانب الأشكال الأخرى للقوة، فعلى سبيل المثال تعرض ما يقرب من 1200 موقع أمريكي لهجمات من قراصنة صينيين في الفترة من 30 أبريل وحتى 7 مايو 2001، وقد شملت تلك الهجمات مواقع البيت الأبيض والقوات الجوية الأمريكية ووزارة الطاقة الأمريكية[3]، وذلك على خلفية اصطدام مقاتلة صينية من طراز "J-8 land" مع طائرة تجسس أمريكية من طراز "EP-3E" فوق جزيرة "هاينان" الصينية في الأول من أبريل 2001، والذي نتج عنه تحطم الطائرة الصينية وغرقها وفقدان طيارها وهبوط الطائرة الأمريكية اضطراريا في مطار جزيرة "هاينان" الصينية، وقد تسببت هذه الحادثة في نشوب أزمة سياسية بين الصين والولايات المتحدة الأمريكية[4]، وقد دفعت هذه الهجمات الإلكترونية

1- عادل عبدالصادق، "القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني"، **مجلة السياسة الدولية**، عدد رقم (188)، (مركز الأهرام للدراسات السياسية والاستراتيجية، أبريل 2012)، ص ص 44 -45.

2-**The Evolution of U.S. Cyberpower,** (The Armed Forces Communications and Electronics Association (AFCEA),P 28,http://www.afcea.org/committees/cyber/documents/TheEvolutionofUSCyberpower.pdf On 23 Feb.

3- Michael A. Vatis, **Cyber Attacks During The War On Terrorism:A Predictive Analysis,** (Institute For Security Technology Studies At Dartmouth College, September 2001), p8.

4- طائرة التجسس الأمريكية في قبضة الصين، مقال موجود على موقع **مجلة الطيران والدفاع**، عدد 35، بتاريخ دخول 20 فبراير، 2012، يمكن مطالعته على الرابط التالي:
http://www.aviadef.com/article.aspx?magid=35&artid=96

إلباستحداث وزارة للأمن الداخلي في الولايات المتحدة التي تم إنشاؤها في نوفمبر 2002 وما أعقبها من إصدار قانون الأمن الوطني (الباتريوت ACT)[1].

ج- تم إنشاء لجنة تحقيق عام 2001 من قبل البرلمان الأوروبي اتهمت الولايات المتحدة الأمريكية باستخدام شبكة إلكترونية منذ الحرب الباردة للتجسس على الصناعات الأوروبية لصالح الشركات الأمريكية[2].

د- يمثل عام 2012 نهاية الفترة الأولى لباراك أوباما، حيث احتلت الولايات المتحدة خلال تلك الفترة المرتبة الثانية في مؤشر القوة الإلكترونية Cyber Power Index[3]، يضاف إلى ذلك تزايد استخدام الولايات المتحدة لقوتها الإلكترونية، خاصة تجاه منشآت إيران النووية في ظل تصاعد الهجمات الإلكترونية الإيرانية على مؤسسات مالية وأنظمة حكومية وشبكات للطاقة الأمريكية[4]، مما دفع وزير الدفاع الأمريكي ليون بانيتا لوصفها بأنها تشبه اعتداء الحادي عشر من سبتمبر 2001 أو الاعتداء الياباني على بيرل هابر (1941[5].

هـ - كشفت شركة "كاسبرسكي لاب" الروسية، المتخصصة في حلول وتطبيقات الأمن والحماية، عن ما تقول إنه أدلة دامغة على وجود تعاون في مرحلة واحدة على الأقل بين البرمجية الخبيثة لفيروس "فليم" (Flame)[6]، وبرمجية فيروس "ستاكسنت" (Stuxnet)[7]، الذي يعتقد على نطاق واسع أن الولايات المتحدة وإسرائيل استخدمتاه

1- Franklin D. Kramer, Stuart H. Starr, Larry Wentz,eds, **Cyberpower and National Security**, Washington D.C: National defense University, May 2009. p 86-172-317
2- Franklin D. Kramer, Stuart H. Starr, Larry Wentz,eds, **Cyberpower and National Security**, Op. cit.P 423

3- يهتم مؤشر القوة الإلكترونية بدراسة عناصر القوة الإلكترونية والأمن الإلكتروني لمجموعة الدول الـ 20 الاقتصادية، ويتكون من 40 مؤشراً تعكس درجة القوة الإلكترونية لهذه الدول وعناصر القوة ومواطن الضعف بها.

4- جريدة الأهرام، 12 أكتوبر 2012.

5- Niall Green, **US Defense Secretary warns of "Pearl Harbor"cyber attack by Iran** ,Onhttp://www.wsws.org/en/articles/2012/10/iran-o15.htmlOn 15 Oct. 2012.

6- فيروس "flame" صمم لسرقة المعلومات من الأنظمة المُستهدفة، مثل معلومات النظام والملفات المخزنة بداخله، والمحتويات التي تعرضها شاشة الحاسوب وحتى المحادثات الصوتية، وحجم هذا الفيروس يفوق بأكثر من عشرين ضعفاً لحجم فيروس "ستاكسنت" الذي استهدف المنشآت النووية الإيرانية عام 2010، بحسب كاسبرسكي لاب.

7- يعد برنامج ستاكسنت جزءاً من برنامج ذاتي الاستنساخ ينتشر من كمبيوتر إلى آخر ضرب المنشآت النووية الإيرانية في عام 2010 حيث أعلنت الاستخبارات الإيرانية أن هذا الفيروس أصاب ما يقدر بستة عشر ألف جهاز كمبيوتر، وتبنت إسرائيل المسؤولية عن شن هجمات ستاكسنت بالتعاون مع الولايات المتحدة للعمل على تعطيل المنشآت النووية كجزء من منصة لإطلاق الفيروسات الخطرة تم تطويرها عام 2007 وتمت تجربتها في إسرائيل.

لمهاجمة منشآت الطاقة الإيرانية، ويعتقد أن إيران هي الجهة الرئيسية التي يستهدفها الفيروس، إذ يأتي الإعلان بعد شهر فقط على تأكيد إيران أنها أوقفت انتشار فيروس يمحو بيانات خوادم أجهزة الكمبيوتر في قطاعها النفطي[1].

و- تسمح هذه الفترة بمقارنة احتمالات التغير في العقيدة والاستراتيجية الأمريكية حول استخدام القوة الإلكترونية في ظل رئاسة ديمقراطية وأخرى جمهورية.

وتتمثل الأهمية الرئيسية لهذه الدراسة في محاولة التأصيل النظري باللغة العربية لمفهوم حديث نسبياً وهو مفهوم القوة الإلكترونية، وكيفية استخدامها في مجال العلاقات الدولية، بما يؤدي إلى إثراء المكتبة العربية فيما يتعلق بأبعاد التحول في مفهوم القوة وأشكالها، بالإضافة إلى محاولة لفت نظر صانع القرار العربي إلى نمط جديد من التهديدات هو التهديدات القادمة عبر الفضاء الإلكتروني، وفي نفس محاولة استخدام وتطبيق نمط جديد من أنماط القوة يمكن أن تساعد في تحقيق أهداف الدولة سواء كانت داخلية أو خارجية هو القوة الإلكترونية، والتي يمكن توظيفها في إدارة التفاعلات الدولية، إلى جانب كل من القوة الصلبة سواء العسكرية أو الاقتصادية وكذلك القوة الناعمة. وقد تطرقت بعض الدراسات، خاصة باللغة الإنجليزية إلى مفهوم القوة الإلكترونية.

وقد تم تقسيمها إلى محورين، يتناول الأول منها الأدبيات التي حللت أبعاد التحول في مفهوم القوة، بينما يتعلق الثاني بالدراسات التي تناولت استخدام القوة الإلكترونية في التفاعلات الدولية، خاصة من جانب الولايات المتحدة الأمريكية.

1- فيروس معلوماتي جديد يستخدم "سلاحا إلكترونيا" ضد إيران، **موقع فرنسا 24**، بتاريخ دخول 29 مايو 2012 http://www.france24.com/ar/20120529-فيروس-معلوماتي- جديد- استخدام - سلاح - إلكتروني-إيران-إسرائيل- الولايات- المتحدة – الأمريكية – البرنامج – النووي 20%.

أولاً: الدراسات المتعلقة بأبعاد التحول في مفهوم القوة والتغيرات النظرية التي طرأت عليه:

شهدت ستينيات القرن الماضي مولد فكرة اتصال أجهزة الحاسب ببعضها البعض من خلال شبكة تستخدم تكنولوجيا مختلفة عن تلك المستخدمة في أنظمة الهاتف، وهذه الفكرة تحديداً تبنتها وكالة الأبحاث المتطورة التابعة لوزارة الدفاع الأمريكية ونتج عنها أول شبكة حاسبات في التاريخ والمعروفة باسم "أربانت" Arpanet، وقد مثلت الأربانت النواة الأساسية للشبكة العالمية المعروفة باسم الإنترنت، وأثناء تطوير الأربانت لم يكن يخطر ببال الباحثين أنهم يضعون بذلك نواة لأهم الاختراعات البشرية في القرن العشرين، حيث كان كل ما يفكر فيه هؤلاء الباحثون هو بناء شبكة معلومات تستخدم لأغراض البحث العلمي. وكان لهذه الشبكة أثر كبير على مفهوم القوة وتحولاتها، وقد جادل جوزيف ناي بأن قدرة الدولة على توظيف قوتها الصلبة والناعمة لتحقيق أهدافها يخلق نوعاً جديداً من القوة هو "القوة الذكية"، ولما كان للتكنولوجيا أثر على مفهوم القوة وتحولاتها، خاصة مع بروز الفضاء الإلكتروني، أصبح لدينا مفهوم جديد للقوة وهو "القوة الإلكترونية"، **وفيما يلي بعض الأدبيات التي تعرضت للفضاء الإلكتروني والقوة الإلكترونية:**

يعتبر جوزيف ناي أهم منظري مفهوم القوة الإلكترونية، والتي قدم أكثر من دراسة تقترب من هذا المفهوم وتتناوله منها "مستقبل القوة"، "القيادة والقوة الناعمة والقوة الصلبة"، و"القوة الإلكترونية".

حيث تناقش الدراسة الأولى قدرة الدولة على ممارسة التأثير على المستوى الدولي من خلال استخدامها القوة الصلبة المتمثلة – غالباً – في القوة العسكرية، أو القوة الناعمة المتمثلة في الجاذبية الثقافية والقدرة على الإقناع، ويجادل ناي بأن كلاهما مهم لزيادة قوة الدولة وقدرتها على التأثير في الآخرين، وأن القدرة على تحقيق التوازن بين هاتين القوتين أطلق عليه ناي اسم القوة الذكية، كما قدم جوزيف ناي في كتابه بعض التحليلات الخاصة بالتراجع النسبي للولايات المتحدة كقوة عظمى في مواجهة الصين. حيث يجادل بأنه ليس من الضروري أن تحدث حرب صدامية بين

الولايات المتحدة والصين في القرن الحادي والعشرين إذا استطاعت كل منهما أن تتعاونا سوياً في عدد من المجالات، بدايةً من تحقيق الاستقرار الاقتصادي على المستوى الدولي، وانتهاء بمواضيع أخرى، كالتغيرات المناخية وغيرها من القضايا المطروحة على الساحة الدولية، وقد اعتمد جوزيف ناي في تحليلاته على دراسته السابقة حول القوة الصلبة والقوة الناعمة، فكل من الصين والولايات المتحدة يمتلك هذين النوعين من القوة وإن كان بدرجات مختلفة، وأن تعاونهما سوياً يحقق النوع الآخر من القوة هو القوة الذكية[1].

أما في الدراسة الثانية فقد تناول ناي التغيرات التي طرأت على خصائص القيادة سواء كانت سياسية أو غيرها، نتيجة لثورة المعلومات، خاصة في الدول التي تعدت مرحلة الثورة الصناعية، وتطرق إلى مفهوم القوة، حيث أشار إلى أن القوة تعني القدرة على التأثير في سلوك الآخرين للحصول منهم على النتائج التي يريدها القائم بعملية التأثير، ويمكن تحقيق ذلك إما من خلال الإكراه أو الإغراء أو الجذب، ويجادل بأن القوة الناعمة تكمن في القدرة على ترتيب وتشكيل أولويات الآخرين، ويعتمد ذلك على بعض الإمكانيات غير المادية كالقيم والجاذبية الشخصية، في حين تعتمد القوة الصلبة على الإكراه أو التهديدات أو الإغراءات، ويرى ناي أن المزج بين هاتين القوتين ينتج عنه ما سماه القوة الذكية، وقد خلص ناي إلى نتيجة مهمة مفادها تغير متطلبات وخصائص القيادة، فلم تعد القوة الصلبة هي العامل الرئيسي للقيادة، كما أن القوة الناعمة بمفردها عاجزة عن تحقيق قيادة ناجحة، وإنما درجات متفاوتة من كلا القوتين، والقيادة الذكية هي التي تستطيع الخروج بمصفوفة من هاتين القوتين تستطيع من خلالها تحقيق أهدافها[2].

وفي الدراسة الثالثة، حلل ناي مفهوم القوة الإلكترونية Cyber power طارحاً عدة ملاحظات أبرزها مظاهر حوسبة الحياة البشرية والدور المتصاعد للحاسب الآلي، وكيف أثر التطور التكنولوجي على مفهوم القوة بداية من اختراع الطباعة وانتهاء

1- Joseph Nye, **The Future of Power**, (Harvard University, 10 May 2011).
2- Joseph S. Nye, **Soft Power, Hard Power and Leadership**, (Harvard University, October 2006), For more details:
http://www.hks.harvard.edu/netgov/files/talks/docs/11_06_06_seminar_Nye_HP_SP_Leadership.pdf

باختراع الإنترنت، والدور الذي تلعبه كإحدى أدوات الصراع الدولي، وتطرق إلى متطلبات القوة الإلكترونية Cyber power والتي تتمثل في بنية معلوماتية، وأجهزة إلكترونية تساعد على التحكم في الاتصالات وربط أجهزة الكمبيوتر ببعضها البعض، وبرمجيات Soft Ware، ومهارات بشرية مدربة للتعامل مع هذه التكنولوجيا، ثم تعرض لخصائص الفضاء الإلكتروني، والتي من أبرزها البعد الاقتصادي والمتمثلة في انخفاض تكلفة امتلاكه واستخدامه، والبعد المعلوماتي، فضلاً عن كونه بيئة من صنع الإنسان وليس كالأرض أو البحر أو الفضاء الخارجي، ثم عامل السرعة والتطور الذي يتميز به وزيادة عدد الفاعلين المستخدمين له واختلاف تصنيفاتهم ثم إمكانية التخفي من خلاله، كما تعرضت الدراسة لخصائص الصراع في الفضاء الإلكتروني ووجوه استخدام القوة في الفضاء الإلكتروني والأبعاد الرئيسية للأمن القومي، انطلاقاً من دور الإنترنت واستخداماتها[1]، إلا أن الدراسة لم تهتم بالتأصيل النظري لمفهوم القوة الإلكترونية أو تشير إلى نظرية حاكمة للقوة الإلكترونية.

بينما حللت سعاد محمود في دراستها بعنوان"دورة القوة: ديناميكيات الانتقال من الصلبة إلى الناعمة إلى الافتراضية"أبعاد التحول في مفهوم القوة والسياق الفكري الذي صيغ في إطاره حجم التغير الذي أدخل على المفهوم من جانب المدارس المختلفة في العلاقات الدولية، وكذلك تأثير الثورة المعلوماتية علي مفهوم القوة من حيث العناصر المكونة للقوة وأشكالها، ومن ثم تطور القوة من الصلبة إلى الناعمة إلى الافتراضية، وتصل لنتيجة مفادها أن مفهوم القوة من المفاهيم الخلافية التي تتسم بالتعقيد، ولا يرجع ذلك فقط لتعدد أبعاد القوة والتطور في أشكالها، ولكن أيضاً لتعقد القضايا المرتبطة بها وتباين مصادر التهديد في السياسة الدولية، وتجاوزها حدود الدولة القومية، هذا فضلاً عن تعدد الفاعلين وانتشار القوة[2].

وحاول علي جلال في دراسته بعنوان "إعادة انتشار القوة: تحليل أولي لأبعاد وآثار انتشار القوة داخل وبين الدول"تقديم قراءة أولية في مفهوم انتشار القوة، وأبعاده، من خلال التعامل مع القوة على أنها تعني السلطة، وذلك عند الحديث عن انتشار القوة داخل الدولة، أو إعادة انتشارها بفعل الثورات، وعلى أنها تعني قوة الدولة في مواجهة الفاعلين الآخرين في العالم، عند الحديث عن انتشار القوة في النظام الدولي، حيث تميز الدراسة بين هذين المستويين لانتشار القوة لأغراض تحليلية،

1- Joseph S. Nye, **Cyber Power**, (Harvard Kennedy School, May 2010).

2- د. سعاد محمود، **مرجع سبق ذكره**، ص ص 13- 17.

فعملياً هناك تداخل بينهما، فمن ناحية لا ينتج تراجع دور الدولة في الداخل فقط من تزايد دور الفاعلين المحليين الآخرين داخلها، وإنما ينتج أيضاً عن انتشار القوة بين الفاعلين الخارجيين، سواء كانوا من الدول أو من غير الدول، وما يترتب على ذلك من تزايد دورهم في المجالات الداخلية المحجوزة تقليدياً للدولة. ومن ناحية أخرى يمتد تأثير الفاعلين المحليين من غير الدول إلى الخارج بما يسهم في إنهاء احتكار الدولة لدور الفاعل الوحيد في العلاقات الدولية، وفي النهاية تكشف هذه الدراسة عن تعدد مظاهر انتشار القوة ومستوياتها، وتعدد آثار الانتشار الإيجابية والسلبية[1].

في حين تعرض عادل عبدالصادق في دراسته بعنوان "القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني" لبعض التحديات التي طرحها الفضاء الإلكتروني على الساحة الأكاديمية، والخاصة بإعادة تعريف الأمن والقوة والصراع، حيث قام الكاتب باستعراض علاقة الفضاء الإلكتروني بإحداث تغييرات في البيئة الأمنية الدولية، وكيف أثر في مفهوم القوة وأنماط استخدامها، وبروز أنماط جديدة للصراع الدولي، حيث يرى الكاتب أن هذه القضايا تطرح سؤالاً مهماً حول سباق تسلح إلكتروني، وكيفية وضع حد لهذا التسلح، ثم يختتم الدراسة بالتحديات التي تواجه الأمن العالمي في عصر الفضاء الإلكتروني، ويقدم توصية بضرورة التعاون الدولي، وفتح الطريق للتعاون المثمر بين الحكومات والأفراد والشركات في مجال تكنولوجيا الاتصال والمعلومات لمواجهة هذه التحديات[2]، إلا أن الكاتب أولى اهتماماً أكبر لأثر الفضاء الإلكتروني على الحروب الإلكترونية، وأغفل أثر الفضاء الإلكتروني على القوة الناعمة، أو كونه مجالاً لتحقيق التقارب والتعاون بين الشعوب كسيناريو بديل لسيناريو الحرب الإلكترونية.

واستفاد الكاتب من هذه الأدبيات السابقة في إعداد دراسته، خاصة ما يتعلق بمفهوم القوة والتطورات التي طرأت على أبعاد وأشكال القوة من الصلبة إلى الناعمة ثم الإلكترونية، كذلك ظاهرة انتشار القوة في العلاقات الدولية وتعدد الفاعلين الدوليين الذين يمارسون القوة في العلاقات الدولية.

1- علي جلال، "تحليل أولي لأبعاد وآثار انتشار القوة داخل وبين الدول"، **مجلة السياسة الدولية، ملحق اتجاهات نظرية، القوة: كيف يمكن فهم تحولات القوة في السياسة الدولية؟**، العدد 188، (أبريل 2012)، ص ص 18 – 23.
2- عادل عبدالصادق، "القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني"، **مجلة السياسة الدولية**، العدد 188، (مركز الأهرام للدراسات السياسية والاستراتيجية، أبريل 2012)، ص ص 28- 35.

ثانياً: الدراسات المتعلقة بتوظيف القوة الإلكترونية في إدارة التفاعلات الدولية:

شهد القرن العشرون ثورة معلوماتية كان لها انعكاساتها على مسار السياسة الدولية، حيث أفرزت تلك الثورة ثلاثة عناصر أساسية هي المعلومة، والفضاء الإلكتروني، والطابع الرقمي، ويمكن التمييز بين ثلاثة أبعاد لتأثير الثورة المعلوماتية في السياسة الدولية، يتمثل البعد الأول في ظهور شكل جديد من القوة هو القوة الإلكترونية، ويتمثل البعد الثاني في تغير أدوات شن الحروب، ويتمثل البعد الثالث في الانتشار العنكبوتي للقوة، وقد طور جوزيف ناي نموذجاً حول العلاقة بين القوة الإلكترونية والأشكال الأخرى من القوة سواء الصلبة أو الناعمة.

وقد تطرقت بعض الأدبيات لتوظيف القوة الإلكترونية في التفاعلات الدولية، خاصة الولايات المتحدة الأمريكية ومنها:

دراسة محمد عبدالسلام بعنوان "استخدامات القوة: كيف يمكن التأثير في سلوك الفاعلين الدوليين" حيث تشير إلى أن الدول تستخدم أساليب متعددة بأشكال معقدة للتأثير في سلوك الدول الأخرى، وتحيط بكل منها أطراف سياسية مختلفة، تحدد ما يستخدم منها، وكيفية استخدامه، ويتم ذلك في إطار عملية ديناميكية تتطور وتتصاعد مع الوقت، تبعاً لحيوية الهدف الذي يتم العمل على تحقيقه، فإذا فشل الإقناع تستخدم المكافأة، وإذا لم ينجح ذلك فغالباً ما تستخدم القوة العنيفة المتمثلة في الحرب، وإذا فشلت تبدأ محاولةالانسحاب أو التسوية أو التفاهم مرة أخرى[1]، ويعاب على هذه الدراسة عدم التطرق باستفاضة لمجال استخدامات القوة في العلاقات الدولية بقدر الإسهاب في سلوك الفاعلين الدوليين من خلال دائرة (الإقناع – المكافأة – العنف).

واهتمت دراسة لكارلوس بيلو بعنوان "Cyber Warfare: An Analysis Of The Means And Motivations Of Selected Nation States"بتقييم واقعي لبعض

1- د. محمد عبدالسلام، استخدامات القوة: كيف يمكن التأثير في سلوك الفاعلين الدوليين، **مجلة السياسة الدولية، ملحق اتجاهات نظرية "القوة: كيف يمكن فهم تحولات القوة في السياسة الدولية"**، عدد رقم 180، (مركز الأهرام للدراسات السياسية والاستراتيجية، أبريل 2010)، ص ص 24 -27.

الدول التي تسعى لاستخدام هجمات إلكترونية ضد الولايات المتحدة الأمريكية أو بعض الأعداء الإقليميين لها، وهذه الدول هي الصين، الهند، وروسيا، إيران، باكستان، كوريا الشمالية، وقد خلصت الدراسة إلى أن حكومات ووزارات خارجية الدول الست السابقة تسعى للحصول على إمكانيات حرب إلكترونية، وذلك من خلال جمع المعلومات الاستخبارية، وسرقة البرامج، ومقارنة سلامة البيانات، وإدارة إدراك العدو[1].

وتتناول دراسة لكينث جريس بعنوان " Cyber Space and the changing nature of warfare" خمسة عناصر رئيسية كانت السبب في صعود الحرب الإلكترونية تتمثل في قابلية الإنترنت للهجوم، وعدم كفاية وسائل الدفاع في مجال الفضاء الإلكتروني، وأن له عوائد استثمار مرتفعة، فضلاً عن ظاهرة التخفي عبر الإنترنت وإنكار الشخصيات الحقيقية، وكذلك زيادة مشاركة الجهات الفاعلة غير الحكومية. ثم يعرض الكاتب خمس وسائل أخرى تستخدم في مجال الحرب الإلكترونية وهي التجسس، الدعاية، الحرمان من خدمة الإنترنت، تعديل البيانات والتلاعب بها، والتلاعب أيضاً بالبنية التحتية، وفي النهاية يستعرض الكاتب خمسة نماذج تم استخدام الحرب الإلكترونية فيها وهي روسيا والشيشان عام 1994، ثم تدخل الناتو في حرب كوسوفا عام 1999، والحرب الإلكترونية في الشرق الأوسط عام 2000، والصراع الأمريكي الصيني الذي هاجمت فيه الصين مواقع إلكترونية للولايات المتحدة عام 2001، وأخيراً الحرب الإلكترونية الروسية ضد إستونيا عام 2007. ويصل الكاتب في النهاية إلى نتيجة مفادها أن جميع الصراعات السياسية والعسكرية لها أبعاد إلكترونية[2].

ويتطرق كريستيان لورد في دراسته بعنوان" America's Cyber Future Security and Prosperity in the Information Age" إلى المستقبل الإلكتروني للولايات المتحدة الأمريكية بتحليل مجموعة من العناصر الرئيسية الخاصة بالقوة

1- Charles G. Billo, **Cyber Warfare An Analysis Of The Means And Motivations Of Selected Nation States**, (Institute For Security Technology Studies At Dartmouth College, November 2004).

2 - Kenneth Geers, **Cyber Space and the changing nature of warfare**,(U.S. Representative Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia). On http://www.carlisle.army.mil/DIME/CyberSpace.cfm On Feb 2013.

الإلكترونية للولايات المتحدة الأمريكية وهي: مصالح الولايات المتحدة في الفضاء الإلكتروني، وطبيعة التهديدات التي تواجه هذه المصالح، والجهود التي تبذلها الحكومة الأمريكية لتدعيم الأمن الإلكتروني الأمريكي، ثم يتطرق إلى تحليل العلاقة بين القوة والأمن القومي في الفضاء الإلكتروني، باعتبار أن أحد ملامح القرن 21 هو انعدام الأمن الإلكتروني، خاصة مع تصاعد دور الفاعلين من غير الدول في مجال الصراع الإلكتروني، وانطلاقاً من ذلك سعت هذه الدراسة إلى وضع عدة سيناريوهات للأمن الإلكتروني في المستقبل[1].

أما دراسة ميشيل فاتيس بعنوان " Cyber Attacks During The War On Terrorism A Predictive Analysis" فتتناول بعض حالات الصراع السياسي الذي أدى إلى هجمات على أنظمة الدول الإلكترونية، مثل الصراع بين الهند وباكستان حول إقليم كشمير، والصراع الإسرائيلي الفلسطيني، وتدخل منظمة حلف شمال الأطلنطي الناتو في حرب كسوفو، والصراع بين الولايات المتحدة الأمريكية والصين على خلفية اصطدام طائرة مقاتله صينية بطائرة استطلاع أمريكية انتهت بشن هجمات إلكترونية على الولايات المتحدة الأمريكية، وقد خلصت الدراسة لعدة دروس مستفادة من حالات الدراسة أهمها: أن الهجمات الإلكترونية تصاحبها في العادة هجمات مادية، نحو أهداف ذات قيمة كبيرة[2].

وحللت دراسة ريتشارد كوجلر بعنوان"Deterrence of Cyber Attacks"الأخطار الناجمة عن تهديدات الهجمات الإلكترونية للولايات المتحدة الأمريكية، والتي أصبحت في تزايد مستمر ومن الممكن أن تؤدي إلى خسائر فادحة في شبكات المعلومات الأمريكية، ومن ثم ترى هذه الدراسة أنه إذا استطاعت الولايات المتحدة أن تردع أعداءها عن تنفيذ هجمات إلكترونية ضدها، فإن ذلك من شأنه أن يقلل المخاطر التي يمكن أن تواجهها، مؤكدة أن الردع الإلكتروني يجب أن يعمل على تجميع القدرات المادية والإلكترونية والدبلوماسية والاقتصادية والعسكرية، لمواجهة أعداء الولايات المتحدة، خاصة الصين

1-Kristin M. Lord And Travis Sharp, Editors, **America's Cyber Future: Security And Prosperity In The Information Age**, (Center For A New America Security, June 2011).
2- Michael A. Vatis,**Cyber Attacks During The War On Terrorism: A Predictive Analysis**,(Institute For Security Technology Studies At Dartmouth College, September, 2001).

التي تقوم بشن هجمات إلكترونية ضد الولايات المتحدة، كما تتناول الدراسة أيضاً كيف ترى الوثائق الرسمية الأمريكية تهديدات الإنترانت، كما تشرح كيف يمكن التعامل مع التهديدات الإلكترونية ودور الردع في مواجهة هذه التهديدات، وتصل الدراسة لنتيجة مفادها حاجه الولايات المتحدة لوضع استراتيجية ردع إلكتروني، نظراً لكون الولايات المتحدة قوة عسكرية، فضلاً عن قابليتها هي وحلفائها لهجمات رئيسية ضد شبكات المعلومات التي تمتلكها وهو ما يهدد مصادر قوتها[1].

وتناقش دراسة إرفينجلاتشو بعنوان "Cyber Terrorism Menace or Myth?" للإرهاب الإلكتروني، وتبدأ بتعريفه، ثم تتعرض للتهديدات الناجمة عن الإرهاب الإلكتروني، وتثير عدة أسئلة حول الإرهاب الإلكتروني، حيث تتساءل لماذا لا يوجد حتى الآن أي حادثة إرهاب إلكتروني ضد الولايات المتحدة، أم أن العملية هي مسألة وقت حتى يتمكن الإرهابيون من تجهيز وإطلاق هجمات إلكترونية ضخمة ضد الولايات المتحدة، وإذا لم يكن الإرهابيون يستخدمون الإنترنت لشن هجمات ضد الولايات المتحدة، فلأي غرض يستخدمون الإنترنت؟ وتؤكد الدراسة أن الإرهابيين لم يستخدموا الإنترنت حتى الآن لإطلاق هجمات إلكترونية ضخمة بقدر ما يتم استخدامه في جمع المعلومات الاستخباراتية وتنسيق الجهود بينهم لشن هجمات ضد أهداف مادية مثل البنية التحتية. وتصل الدراسة لعدة نتائج منها أهمية أن تعمل الولايات المتحدة على منع الجماعات الإرهابية من استخدام الإنترنت في تجنيد عملاء لها أو استخدمها في التنسيق بين هذه الجماعات أو بعضها البعض(2).

في حين تتعرض دراسة تيموثي توماس بعنوان "Nation-state Cyber Strategies Examples from China and Russia" لنماذج واقعية لاستخدام كل من الصين وروسيا للقوة الإلكترونية في السياسة الخارجية والصراع الدولي، حيث يشير الكاتب Timothy L. Thomas إلى اتهام الصين بشن العديد من الهجمات

1-Richard L. Kugler, "Deterrence of Cyber Attacks", in Franklin D. Kramer, Stuart H. Starr, Larry Wentz , eds, **Cyberpower and National Security**,(Washington D.C: National defense University, May 2009), p p 309 -337.

2-Irving Lachow, "Cyber Terrorism: Menace or Myth?", D. Kramer, Stuart H. Starr, Larry Wentz ,eds, **Cyberpower and National Security**, (Washington D.C: National defense University, May 2009), p p 437- 464.

الإلكترونية المقصودة ضد العديد من دول العالم، خاصة الولايات المتحدة الأمريكية، حيث شنت الصين هجمات إلكترونية ضد أجهزة الكمبيوتر الخاصة بوزارة الدفاع الأمريكية في عام 2005، فضلاً عن محاولة إعاقة أجهزة الأقمار الصناعية الأمريكية عام 2006 باستخدام هجمات ليزر عالية، وكذلك الهجوم الإلكتروني ضد كلية البحرية الأمريكية، والذي أغلق البريد الإلكتروني وأجهزة الكمبيوتر لأسابيع عديدة، وإدانتها أيضاً بشن هجمات إلكترونية ضد اليابان وتايوان. ثم يتطرق للحديث عن القوة الإلكترونية في العقيدة الروسية، حيث أعلن الرئيس الروسي فلاديمير بوتن في فبراير 2008 استراتيجية تنمية مجتمع المعلومات الروسي، وشرح المقصود بالقوة الإلكترونية في الاستراتيجية، كما تطرق إلى شن بعض الهجمات الإلكترونية الروسية على إستونيا في 2007 والتي استمرت 3 أسابيع وتسببت في توقف المعاملات البنكية والمصرفية فضلاً عن تدمير كثير من المواقع الرسمية والحزبية في إستونيا، وكذلك الهجوم الإلكتروني ضد جورجيا في 2008 قبل أن يعقبه غزو عسكري، ودور القوة الإلكترونية في تحقيق الأهداف الروسية في هذه المعارك[1].

وتحللدراسة ريبيكا جرانت بعنوان "Victory In Cyberspace" علاقة الفضاء الإلكتروني بمختلف نواحي الحياة خاصة الاقتصادية والعسكرية، حيث ترى أن أهمية الفضاء الإلكتروني أصبحت تتساوى مع أهمية الفضاء الجوي والفضاء الخارجي، وما جعل الفضاء الإلكتروني يحظى بهذه الأهمية هو العمليات الحيوية التي يتم استخدامه فيها سواء العسكرية أو التجارية، وهو ما جعله منطقة صراع من أجل السيطرة عليه، وترى هذه الدراسة أن الحديث عن حرب إلكترونية يكون مجالها الفضاء الإلكتروني ظل حديثاً نظرياً حتى 26 أبريل 2007 حينما تعرضت إستونيا لهجمة إلكترونية شلت معظم القطاعات الحيوية بها، وهو ما يعتبر أول حرب إلكترونية تم استخدام الفضاء الإلكتروني فيها لتدمير أهداف حيوية للعدو. وقد أشارت الدراسة إلى التخوفات الأمريكية من إمكانية تكرار السيناريو الإستوني

1-Timothy L. Thomas,"Nation-state Cyber Strategies: Examples from China and Russia",in Franklin D. Kramer, Stuart H. Starr, Larry Wentz ,eds, **Cyberpower and National Security**,(Washington D.C: National defense University, May 2009). Pp 465 – 490.

معها، خاصة في مجال التعاملات المالية والمصرفية، أو المعلومات العسكرية وبالتالي يتوجب على الولايات المتحدة أن تكون رائدة في هذا المجال لحماية أمنها القومي[1].

وأوضحت دراسة محمد أبو رمان بعنوان "تنظيم القاعدة والإنترنت .. تدشين الجيل الثالث من الجهاديين" كيف استخدم تنظيم القاعدة والتنظيمات الجهادية السلفية – كنموذج للفاعلين من غير الدول – الفضاء الإلكتروني في تنفيذ أهدافها واستقطاب منتمين جدد لها، حيث أشار الكاتب إلى اعتراف الولايات المتحدة بتفوق القاعدة في حربها الإعلامية الإلكترونية، إذ تكاثرت المواقع والمنتديات الجهادية بشكل هائل ومذهل منذ الإعلان عن تأسيس الجبهة العالمية لقتال اليهود والصليبيين عام 1998 من 12 موقعاً لتصل إلى 6000 موقع في 2010، كما أشار الكاتب إلى مفهوم جديد وهو "القيادة الافتراضية" التي تظهر في العالم الافتراضي، مثل أبي بكر الناجي وأبي عبيد الفرشي وغيرهما من القيادات الجهادية السلفية التي تنتمي إلى القاعدة وتستخدم الفضاء الإلكتروني مجالاً لتحركاتها، وعلى الرغم من تراجع دور القاعدة بعد مقتل رئيس التنظيم والأب الروحي أسامة بن لادن، فإن كون القاعدة فاعلاً من غير الدول قادراً على توجيه هجمات للدول يظل نموذجاً واضحاً في إطار مفهوم انتشار القوة وتعدد الفاعلين الممارسين لها[2].

وفي النهاية تحلل دراسة "جيسون سباد" بعنوان " China's Cyber Power And America's National Security" القوة الإلكترونية للصين وتأثير ذلك على الأمن القومي الأمريكي، حيث أشارت إلى أن استخدام شبكات الكمبيوتر والقوة الإلكترونية أصبح مصدر تهديد في الوقت الحالي، خاصة ضد الولايات المتحدة الأمريكية لسهولة استخدامها ورخص تكلفتها، وهو ما قد يدفع أعداء الولايات المتحدة إلى استخدامها ليس فقط في المجال العسكري، ولكن أيضاً في المجال الاقتصادي والسياسي، وقد خلصت الدراسة إلى أنه منذ 1991 وتسعى جمهورية الصين الشعبية لتمويل وتطوير والحصول على تكنولوجيا إلكترونية متطورة في

1- Rebecca Grant, **victory in cyberspace**, An Air Force Association Special Report, October 2007.

2- د.محمدأبورمان، "تنظيم القاعدة والإنترنت .. تدشين الجيل الثالث من الجهاديين"، **مجلة السياسة الدولية**، عدد رقم (180)، (مركز الأهرام للدراسات السياسية والاستراتيجية، أبريل 2010)، ص ص 86 – 91.

المؤسسات الحكومية والعسكرية والمدنية، وذلك لبناء قوة سياسية واقتصادية صينية في مواجهة الولايات المتحدة الأمريكية، وفي إطار ذلك يعد جيش التحرير الشعبي الصيني نفسه لخوض حرب إلكترونية شاملة، من خلال استخدام الإنترنت في جمع المعلومات، والسيطرة على أجهزة الاتصالات والمعلومات، وتدمير البنية التحتية، وإصابة الاقتصاد القومي الأمريكي بأضرار جسيمة، كتمهيد لخوض صراع مسلح، مدعمة وجهة نظرها بطرح تجارب واقعية، مدعمة وجهة نظرها بطرح تجارب واقعية لاستخدام الصين للقوة الإلكترونية ضد بعض الدول، مثل تايوان في 2005، وألمانيا في 2007[1].

ويستفيد الكاتب من هذه الأدبيات السابقة في معرفة عناصر القوة الإلكترونية الأمريكية، والمصالح الأمريكية ومصادر التهديد لها في الفضاء الإلكتروني، وكذلك حدود القوة الإلكترونية الأمريكية والقيود المفروضة عليها، فضلاً عن معرفة بعض حالات استخدام القوة الإلكترونية في التفاعلات الدولية، سواء سياسية أو عسكرية أو اقتصادية، وهو ما يخدم الكاتب في فهم توظيف القوة الإلكترونية الأمريكية في التفاعلات الدولية.

إقتراب نظري:

استخدم الكاتب في تحليله لاستخدام القوة الإلكترونية في التفاعلات الدولية إطاراً نظرياً يرتكز على مفهوم القوة كما توظفه كل من المدرسة الواقعية والمدرسة الليبرالية، حيث إن الاستخدام الفعلي للقوة الإلكترونية في السياسة الدولية يتم في إطار الجمع بينها وبين كل من القوة الصلبة والقوة الناعمة، حيث يعتمد الكاتب في هذا الإطار على النموذج الذي قدمه جوزيف ناي والذي جمع بين القوة الإلكترونية وكلاً من القوة الصلبة والقوة الناعمة، حلل خلاله كيفية استخدام آليات معلوماتية لتوليد قوة صلبة وناعمة.

1-Colonel Jayson M. Spade, **China's Cyber Power andAmerica's National Security**, Edited By Jeffrey L. CatonU.S. (Army War College 2001).

نموذج "جوزيف ناي" في توظيف القوة الإلكترونية إلى جانب القوة الصلبة والناعمة:

يعرف جوزيف ناي القوة الإلكترونية بأنها القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء الإلكتروني، أي أنها القدرة على استخدام الفضاء الإلكتروني لخلق مزايا، والتأثير في الأحداث المتعلقة بالبيئات الواقعية الأخرى وذلك عبر أدوات إلكترونية[1]. ويجادل ناي بأن مفهوم القوة الإلكترونية يشير إلى مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الإلكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل[2].

وتتعدد أدوات ممارسة القوة في العلاقات الدولية وفقاً لقدرات وإمكانيات ورغبات القوى المشاركة فيه، فقد تكون القوة العسكرية من أهم هذه الأدوات، وقد تكون القوة الاقتصادية والحصار الاقتصادي والمالي هما العامل الرئيسي للسيطرة على الخصم وممارسة القوة عليه، وقد تكون الأداة المعلوماتية من خلال وسائل الاتصال والتكنولوجيا الحديثة والإنترنت هي العامل الرئيسي لحسم صراع بين دولتين.

ويجادل جوزيف ناي بأن هذه الفترة ليست الأولى التي يتأثر مفهوم القوة فيها بالتطور التكنولوجي، فلقد تأثر العالم في القرن الخامس عشر باختراع الطباعة وما أحدثه من تطور في الإصلاح داخل أوروبا من خلال سهولة وصولها إلى الناس واستخدامها. ويضيف أن الثورة التكنولوجية الحالية في بعض الأحيان تتم تسميتها بالثورة الصناعية الثالثة التي تعتمد على صناعة متطورة وسريعة لأجهزة الكمبيوتر والاتصالات ونظم المعلومات والبرامج الحاسبية، والتي أثرت بصورة دراماتيكية على صناعة وخلق ونقل المعلومات[3].

ويرى جوزيف ناي أن الدولة سوف تظل هي الفاعل المهيمن على الفضاء الإلكتروني، ولكن هناك فواعل أخرى سوف تشاركها في هذا الفضاء الإلكتروني

1- Joseph S. Nye, Cyber Power, **Op. Cit**. p4.
2- Ibid 3.
3-Ibid 1-3.

وسوف تجد صعوبة في السيطرة عليه، فالحكومات قلقة من حالة تسرب المعلومات وتدفقها وصعوبة السيطرة عليها.

ويرى أيضاً أن القوى الكبرى ليست لها المساحة نفسها التي يمكن من خلالها السيطرة على الفضاء الإلكتروني مقارنة بقدرتها على السيطرة على الإقليم البحري أو البري. وأن الكيانات الافتراضية التي تنشأ عبر الإنترنت تستطيع أن تلتقي في إقليم افتراضي جديد خاص بها عبر الإنترنت وتنشأ لها كيانات تنظيمية، ومن ثم يتراجع دور الدولة المركزية في حياة البشر. ويضيف أن الدول الكبرى التي تمتلك القوة الصلبة أو الناعمة قبل الولايات المتحدة وجدت نفسها تواجه مشاكل في السيطرة على حدودها على الإنترنت.

ويؤكد أن الفضاء الإلكتروني لن يزيل سيادة الدولة أو حدودها الجغرافية ولكن سوف يؤثر على مفاهيم القوة وتحولات القوة وأدواتها.

وقد حدد ناي أنماطاً لاستخدام القوة الإلكترونية وميز بين الاستخدام الناعم لها والاستخدام الصلب، ويتضح ذلك في التالي:

1- قدرة الفاعل (أ) على التأثير في سلوكيات الفاعل (ب)

ودفعه للقيام بأعمال لم يكن ليقوم بها، وتكون القوة الإلكترونية في هذه الحالة مصدراً للقوة الناعمة كما في حالة اتجاه الدولة لوضع معايير ملزمة للبرمجيات أو استخدام الجماعات الإرهابية للفضاء الإلكتروني في تجنيد بعض الشباب، بينما يكون استخدام القوة الإلكترونية بطريقة استخدام القوة الصلبة ذاتها من خلال الحرمان من خدمة الإنترنت، أو قطع خدمات الإنترنت عن الدولة كاملة، فعلى سبيل المثال تعرضت إستونيا عام 2007 لهجمات افتراضية، استهدفت بنيتها المعلوماتية. كما تم استخدام القوة الإلكترونية لاستهداف القوة الصلبة لدول أخرى، من خلال نشر فيروسات تدمر أجهزة الدولة، وتستهدف نظم الكمبيوتر الخاصة بالخدمات الحكومية[1].

1- Joseph s.Nye, **The Future of Power**, speech before Pacific Forum, March 2011.

2- قدرة الفاعل الدولي على التحكم في أجندة الآخرين:

من خلال إقصاء بعض استراتيجياتهم، من خلال أن يقوم الفاعل (أ) بمنع تنفيذ أجندة الفاعل (ب) من خلال العمل على إقصاء بعض استراتيجياته، ويتضح استخدام الفضاء الإلكتروني في ممارسة القوة الصلبة في هذا الوجه عندما منعت الحكومة الإيرانية عام 2010 – في أعقاب الاحتفال بعيد الثورة الإيرانية – بعض الناشطين السياسيين من عرض فيديوهات على موقع اليوتيوب مضادة للنظام الحاكم، حيث عمدت الحكومة إلى إبطاء سرعة الإنترنت وإعاقة بث هذه الفيديوهات، وبالتالي عملت على إقصاء إحدى استراتيجيات المعارضة الإيرانية في التعبير عن آرائها، ومن مظاهر استخدام الفضاء الإلكتروني لممارسة القوة الناعمة بعض الشروط التي تضعها منظمة الأيكان على أسماء نطاقات الإنترنت، وكذلك المعايير الموضوعة، والتي لاقت قبولاً واسعاً لتصميم واستخدام البرمجيات[1].

3- ترتيب أولويات الفواعل الأخرى

وذلك من خلال أن يقوم الفاعل (أ) بترتيب أولويات الفاعل (ب)، ومن أمثلة ممارسة القوة الصلبة قيام بعض الدول، مثل الصين والسعودية بحجب بعض المواقع ونزع شرعيتها لدى المواطنين وترك مواقع أخرى مفتوحة لهم، وكذلك قيام الولايات المتحدة الأمريكية باتخاذ عدة إجراءات ضد شركات بطاقات الائتمان لمنع ممارسة القمار عبر الإنترنت، بينما من أمثلة القوة الناعمة العمل على نشر أو تقييد قيم وثقافات عبر الإنترنت مثل تطوير قيم رافضة لنشر الإباحية عبر الإنترنت[2].

وبالتالي أصبحت القوة الإلكترونية حقيقة أساسية في العالم بكل مظاهرها المتنوعة، وبما عمل على دعم ومساندة العمليات الحربية والاقتصادية والسياسية، حيث برز مجتمع المعلومات الدولي والاقتصاد الإلكتروني الجديد الذي أثر على طبيعة النظام الدولي، والعمل على توزيع الموارد الاقتصادية ومستويات النمو الاقتصادي

1- Joseph S. Nye, Cyber Power, **Op. Cit**, p 7 -9.
2- Ibid, p 9.

وأنماط التفاعل بين القوى الاقتصادية الدولية، والتأثير على القوة السياسية بالتأثير في عمليات صنع القرار في النظام الدولي[1].

وقد اعتمد الكاتب على عدد من المفاهيم المحورية الحاكمة للدراسة والتي يجب توضيحها في البداية وهي:

الفضاء الإلكتروني Cyber Space:

عرف جوزيف ناي الفضاء الإلكتروني "نطاق تشغيلي محكم باستخدام الإلكترونيات لاستكشاف المعلومات عبر أنظمة مترابطة ببعضها البعض وببنية تحتية لها"[2].

وعرف فريق جامعة الدفاع الوطني الأمريكية الفضاء الإلكتروني عباره عن:

"مجال تشغيلي تجري فيه مجموعة من العمليات ذات الطابع الإلكتروني، ويتميز بأنه ذو طابع فريد ومتفرد، محكم بمجموعة من الاستخدامات التي تعتمد على الإلكترونيات والأطياف الكهرومغناطيسية لإنشاء وتخزين وإبدال وتبادل واستغلال المعلومات من خلال مجموعة من نظم المعلومات المترابطة والمتصلة عبر الإنترنت والبنى التحتية الخاصة به"[3].

ويرتبط بالمفهوم السابق مفهوم آخر هو "حرب الفضاء الإلكتروني" والتي تعد جزءاً من عمليات المعلومات التي يمكن أن يتم استخدامها في مستويات ومراحل الصراع المختلفة سواء كان ذلك على الجانب التكتيكي أو العملياتي أو الاستراتيجي، ويتم استخدام تلك الهجمات في أي وقت سواء أكان وقت سلم أم حرب أم أزمة. وتعرف كليات الحرب الأمريكية الإرهاب الإلكتروني، وتدعوه بهجمات الشبكات

1- عادل عبدالصادق، "مصر ومجتمع المعلومات: هل يمكن تكرار التجربة الهندية؟"، **مجلة تعليقات مصرية**، العدد 17، (مركز الدراسات السياسية والاستراتيجية بالأهرام، يوليو 2004).

2-Joseph Nye, Cyber Power, **Op. Cit**, p3.

3-Daniel T. Kuehl, "**From Cyber Space to Cyber Power: Defining the problems**", in Franklin D. Krammer, Stuart Starr, and Larry K. Wentz. Eds, cyber power and national security (Washington, D.C: National defense up, 2009, p 48.

الكمبيوترية، وتصنفه تحت بند العمليات الإلكترونية. ويتضمن التعريف أن الحرب الرقمية هي الإجراءات التي يتم اتخاذها للتأثير بشكل سلبي على المعلومات ونظم المعلومات، وفي الوقت نفسه الدفاع عن هذه المعلومات والنظم التي تحتويه[1].

القوة الصلبة Hard Power:

تتألف القوة الصلبة من عناصر القوة المادية العسكرية والاقتصادية، وقد ارتبط الحديث عن هذا الشكل للقوة، خاصة القوة العسكرية بفكر المدرسة الواقعية، في حين تبنى جوزيف ناي مفهوماً أوسع للقوة الصلبة لا يقتصر على القوة العسكرية فقط، حيث يرى أنها تعني أيضاً "القدره على استخدام الجزرة عن طريق الأدوات الاقتصادية بهدف التأثير في سلوك الآخرين" وبالتالي يمكن التمييز بين مكونين للقوة الصلبة، يتمثل المكون الأول في القوة العسكرية، وتعد من أكثر أشكال القوة الصلبة تقليدية واستخداماً، تتراوح بين دبلوماسية الإكراه، والتي تعبر عن أخف استخدامات القوة، إلى الاستخدام المباشر للقوة العسكرية، والتي تعبر عن أكثر الاستخدامات مباشرة ووضوحاً[2].

القوة الناعمة Soft Power:

شهد مفهوم "القوة الناعمة" صعوداً بعد نهاية الحرب الباردة، على الرغم من أن ما يعبر عنه كان موجوداً قبلها وأثناءها، والذي يتجلى في استخدام أدوات الإقناع والاستمالة وليس الضغط والإكراه في إدارة العلاقات الدولية، كأدوات الدبلوماسية

1- عادل عبدالصادق، أمريكا وتشكيل قيادة عسكرية في الفضاء الإلكتروني، **مجلة تعليقات مصرية**، (مركز الدراسات السياسية والاستراتيجية بالأهرام، يوليو 2009). يمكن مطالعة رابط المجلة:

http://acpss.ahram.org.eg/Ahram/2009/7/12/COMM0.HTM

2- Joseph Nye, **Power In The Global Information Age: From Realist ToGlobal**, (New York, Routledge, 2004) p.5.

الشعبية وتوظيف الأبعاد الثقافية والتعليمية والإبداعية أو توظيف المعونات الاقتصادية والمنح الدراسية في إدارة العلاقات الخارجية، والحق أن جوزيف ناي قد بدأ التفكير في هذا الاتجاه منذ السبعينيات بمشاركة زميله أستاذ العلاقات الدولية البارز روبرت كيوهين حين نشرا كتابهما عن "القوة والاعتماد المتبادل: السياسة الدولية في لحظة تحول" عام 1977 الذي تناول فكرة مركزية هي الاعتماد المتبادل غير المتماثل الذي يخلق مساحة للتأثير والنفوذ يمكن في ظلها توظيف أدوات متنوعة للقوة، وقد قام كيوهين بتطوير أفكاره لاحقاً في اتجاه الاقتصاد السياسي، في حين اهتم جوزيف ناي بالإعلام والتعليم وبناء النموذج الثقافي للدولة للتأثير في الفاعلين الآخرين، ودفعهم لتبني سياسات تخدم مصالحها[1].

وقد عرف جوزيف ناي القوة عموماً بأنها: القدرة على التأثير في الأهداف المطلوبة، وتغيير سلوك الآخرين عند الضرورة، وعرف القوة الناعمة بأنها القدرة على الحصول على ما تريد من خلال الإقناع وليس الإكراه ويستبعد من تعريفه العقوبات الاقتصادية والسياسية والعسكرية[2]. حيث أوضح أن "القوة الناعمة هي، في جوهرها، قدرة أمة معينة على التأثير في أمم أخرى، وتوجيه خياراتها العامة، وذلك استناداً إلى جاذبية نظامها الاجتماعي والثقافي ومنظومة قيمها ومؤسساتها بدل الاعتماد على الإكراه أو التهديد". هذه الجاذبية يمكن نشرها بطرق شتى: الثقافة الشعبية، الدبلوماسية الخاصة والعامة، المنظمات الدولية، ومجمل الشركات والمؤسسات التجارية العاملة[3].

وقد ارتبط الحديث عن القوة الناعمة كأحد أشكال القوة بمحاولات جوزيف ناي معالجة التحليل الضيق لمفهوم القوة الذي قدمته المدرسة الواقعية، والذي كان يركز على القوة العسكرية، وقد ميز ناي بين ثلاثة أنماط من القوة الناعمة هي الجاذبية

1- د. هبة رؤوف عزت، **القوة الناعمة المهدرة: أزمة النظام القوي والدولة الضعيفة بمصر**، (مركز الجزيرة للدراسات، أكتوبر 2011)، يمكن مطالعة الدراسة على الرابط التالي:
http://studies.aljazeera.net/files/2011/08/20118872345213170.htm

2- مسعد بن ظافر القحطاني، **استراتيجية توظيف القوة الناعمة لتعضيد القوة الصلبة في إدارة الأزمة الإرهابية في المملكة العربية السعودية**، (جامعة نايف العربية للعلوم الأمنية، الرياض 2010)، ص 8.

3- رفيق عبدالسلام، **الولايات المتحدة الأمريكية بين القوة الصلبة والقوة الناعمة**، (مركز الجزيرة للدراسات، 2008)، ص 8.

Attraction ويشير إلى جذب الانتباه، إما بطريقة سلبية أو إيجابية، والنمط الثاني هو الإقناع Persuasion ويستخدم للتأثير في معتقدات الآخرين وردود أفعالهم دون التهديد باللجوء إلى القوة، وينصرف النمط الثالث إلى وضع جدول الأعمال أو ما يطلق عليه Agenda Setting وتحديد أولويات الدول الأخرى بما يخدم أو يتفق مع أولويات الدولة التي تمارس القوة الناعمة[1].

القوة الإلكترونية Cyber Power:

يعتبر جوزيف ناي من أهم من تحدثوا عن القوة الإلكترونية كشكل جديد للقوة، وهي مرتبطة بامتلاك المعرفة التكنولوجية، والقدرة على استخدامها. وهي تعني القدرة على الحصول على المخرجات المرغوبة من خلال استخدام المعلومات المترابطة إلكترونياً عبر الفضاء الإلكتروني[2]، كما تعني أيضاً استخدام الفضاء الإلكتروني في خلق مميزات والتأثير في الأحداث التي تجري عبر البيئات التشغيلية Operational Environments وعبر أشكال وأدوات القوة المختلفة سواء كانت عسكرية أو اقتصادية أو دبلوماسية أو معلوماتية[3].

وقد حدد ناي ثلاثة أنواع من الفاعلين الذين يمتلكون القوة الإلكترونية يتمثل النوع الأول في الدولة والنوع الثاني في الفاعلين من غير الدول والنوع الثالث هم الأفراد. يتمثل النوع الأول في الدولة التي لديها القدرة على تنفيذ هجمات إلكترونية وتطوير البنية التحتية وممارسة السلطات داخل حدودها، ويتمثل النوع الثاني في الفاعلين من غير الدول ويستخدم هؤلاء الفاعلون القوة الإلكترونية لأغراض هجومية بالأساس إلا أن قدرتهم على تنفيذ أي هجوم إلكتروني مؤثر تتطلب مشاركة وكالات استخباراتية متطورة وفك رموز مشيفرة وعادة لا تمتلك هذه الجماعات إمكانيات

1- ريهام مقبل، "مركب القوة: عناصر وأشكال القوة في العلاقات الدولية"، مجلة السياسةالدولية، **مرجع سبق ذكره**، ص 7.

2-Joseph S. Nye, Jr, **Cyber Power**, https://projects.csail.mit.edu/ecir/wiki/images/d/da/Nye_Cyber_Powe1.pdf On 26 March 2013.

3- Franklin D. Kramer, Stuart H. Starr, Larry Wentzeds, cyber power and national security, **Op.Cit**, p 48.

الدولة نفسها في مجال استخدام القوة إلكترونية، ولكن يمكن أن ينفذ الفاعلون من غير الدول هجمات متنوعة تشمل اختراق مواقع إلكترونية واستهداف أنظمة الاتصالات الدفاعية. وينصرف النوع الثالث إلى الأفراد الذين يمتلكون معرفة تكنولوجية وقدرة على توظيفها وعادة ما تكون هناك صعوبة في الكشف عن هويتهم، كما أنه من الصعب ملاحقتهم[1].

انتشار القوة Diffusion of power:

ويعد جوزيف ناي أبرز المستخدمين لمفهوم انتشار القوة ووفقاً له يرى أن هذه الظاهرة هي أكثر حداثة وغير مألوفة وتفرض تحديات جديدة على الدول، ويعرفها ناي بأنها تزايد القضايا ومجالات التأثير والتفاعل الواقعة خارج نطاق السيطرة الكلية للدولة بما فيها الدول الأكثر قوة مع ظهور فاعلين جدد يتمتعون بصور جديدة من القوة[2].

وهنا يمكن التمييز بين مستويين لانتشار القوة، المستوى الأول ويقصد به السلطة التي تتمتع بها الدولة في مواجهة المواطنين، والمستوى الثاني ويقصد به القوة التي تتمتع بها الدولة في مواجهة الدول الأخرى، وعملياً فهناك تداخل بين المستويين، فمن ناحية لا ينتج تراجع دور الدولة في الداخل فقط عن تزايد دور الفاعلين المحليين الآخرين داخلها، وإنما ينتج أيضاً عن انتشار القوة بين الفاعلين الخارجيين، سواء كانوا من الدول أو من غيرها، وما يترتب على ذلك من تزايد دورهم في المجالات الداخلية المحجوزة تقليدياً للدولة. ومن ناحية أخرى يمتد تأثير الفاعلين المحليين من غير الدول إلى الخارج بما يسهم في إنهاء احتكار الدولة لدور الفاعل الوحيد في العلاقات الدولية[3].

1-Joseph S.Nye, Cyber Power, **Op. Cit**, PP 9-11.
2-Ibid, 1-3.
3- علي جلال معوض، **مرجع سبق ذكره**، ص ص 18 -19.

وفيما يتعلق بالبعد الخارجي لانتشار القوة، هناك اتجاه يبرز سلبيات مثل هذا الانتشار للقوة، باعتباره يهدد استقرار النظام العالمي. فإذا كان النظام ثنائي القطبية، وفقاً للبعض، يتسم بدرجة أعلى من اليقين التي تقلل احتمالات الصراع والحروب، مقارنة بالنظام متعدد الأقطاب، فإن النظام القائم على انتشار القوة يحمل احتمالات أكبر لعدم الاستقرار والصراع بأشكال مختلفة[1].

ولا يمنع ذلك من وجود اتجاه يرى أن انتشار القوة – مثله في ذلك مثل توازن القوى – لا يقوم بالضرورة على التضاد والصراع، بل قد يكون توافقياً تعاونياً، أو قائماً على التكامل. فانتشار القوة أفقياً ورأسياً ينهي الهياكل الهيراركية القائمة على هيمنة الدول القومية، ويخلق تنظيمات شبكية يستمر في إطارها الدور الأساسي للحكومات والدول، لكن مع زيادة مكانة الفاعلين الآخرين غير الرسميين الذين يقوم بعضهم بجانب من أدوار ووظائف الحكومات. ويسهم ذلك في تطوير معايير جديدة للحكم الرشيد، وتقليل سيطرة الحكومات على حياة الأفراد، لاسيما مع زيادة مصادر قوة قطاعات كبيرة من المواطنين، بفعل تمتعهم بالقوة المعلوماتية المرتبطة بتدفق المعلومات وتداولها[2].

التفاعلات الدولية:

هي الأحداث المتتابعة والمترابطة التي تتكون من سلاسل من الأفعال وردود الأفعال من الفاعلين الدوليين تجاه بعضهم البعض، وتكّون هذه التفاعلات النظام الدولي على أساس أن هناك نماذج متكررة ومتماسكة للتفاعل. وتأخذ هذه التفاعلات شكلاً تعاونياً أو صراعياً.

هذه التفاعلات قد لا تكون سياسية مباشرة، ولكنها قد تكون اقتصادية أو فكرية أو رياضية، ودراسة العلاقات السياسية الدولية تهتم بالتفاعلات السياسية المباشرة بحكم طبيعتها، غير أنها تهتم أيضاً بأنواع التفاعلات الدولية الأخرىوإن يكن من منظور سياسي.

1- **المرجع السابق**، ص 22.

2- Joseph S.Nye, **Op. Cit**, P 115.

يلاحظ أن التعريف استخدم تعبير الفاعلين الدوليين وليس الدول، وذلك اتساقاً مع الاتجاه الحديث في دراسة العلاقات الدولية الذي لم يعد يرى في الدول الفاعل الوحيد في النظام السياسي الدولي، إشارة إلى وجود فاعلين آخرين مؤثرين غير الدول، بل وربما بدرجة أكبر بكثير من الدول، ومن أهم هؤلاء الفاعلين المنظمات الدولية وحركات التحرير الوطني التي بلغت مستوى معيناً من القوة، وبعض الشركات الاقتصادية العملاقة التي اصطلح على تسميتها بالشركات المتعددة الجنسية، وهكذا لم يعد الشرط المطلوب توفره في الفاعل لكي يكون دولياً هو "السيادة"، وإنما القدرة على التأثير في المستوى الدولي[1].

التحكم الانعكاسي Reflexive Control:

عرف فلاديمير ليفيبفر Vladimir A. Lefebvre التحكم الانعكاسي بأنه: عملية من شأنها أن يقوم عدو ببث مجموعة من الأسباب إلى الطرف الآخر لدفعه لصنع قرار معين. أو بمعنى آخر، التأثير على عملية اتخاذ القرار الخاصة بالخصم. وقد عرفه كليفورد ريد Clifford Reid بأنه فرع من نظرية السيطرة متعلق بالتأثير على قرارات الآخرين[2].

فالتحكم الانعكاسي هو عملية من شأنها أن يرسل الفاعل المتحكم مجموعة من الدوافع والأسباب إلى العدو المستهدف من أجل التأثير على تصرفاته، وذلك من خلال القدرة على تقليد سلوك وتصرفات العدو بشأن يدفعه إلى اتخاذ قرار غير مفضل له،

1- د. أحمد يوسف أحمد، د. محمد زبارة، **مقدمة في العلاقات الدولية**، (القاهرة، مكتبة الأنجلو المصرية، 1985)، ص ص5-6.

2- Volodymyr N. Shemayve, **Cognitive approach to modeling reflexive control in Socio-Economic system**, http://infosec.procon.bg/v22/Shemayev_ReflexiveControl.pdf On December 10th, 2012.

ومفضل للفاعل المتحكم[1]، ويعتمد التحكم الانعكاسي على عدة عوامل أهمها القدرة التحليلية وسعة الاطلاع والخبرة ومعرفة عامة بنطاق العدو.

كما يشمل التحكم الانعكاسي Reflexive Control الجانب الأخلاقي والنفسي وكذلك الجوانب الشخصية والعادات وأوجه القصور النفسي والمعنوي، وفي حرب يستخدم فيها السيطرة الانعكاسية نجد الفاعل الذي لديه قدرة أكبر على الانعكاسية وتقليد الطرف الآخر والتنبؤ بسلوكه هو الجانب الذي لديه فرصة أكبر على الفوز.

ونضرب مثالاً على ذلك بأنه مثلما يتم استخدام أجهزة تشويش وتضليل في الحروب للسيطرة على الأسلحة أو لضرب أهداف مضللة، يحدث ذلك في الإنترنت حيث تتم السيطرة على أجهزة التعقب والمراقبة، مثل الأقمار الصناعية والرادارات وأجهزة التجسس، ومن ثم توجيهها لأهداف مضللة أو تغذيتها بمعلومات من شأنها التأثير على صانع القرار.

ويرتبط بهذا المفهوم مفهوم آخر وهو سلاح المعلومات Information Weapon، حيث عرفه سيرجي ماركوف[2] بأنه: معلومة محددة قادرة على إحداث تغيير في عملية المعلومات الخاصة بنظام المعلومات المستخدم في صناعة القرار، وفقاً لنوايا الكيان الذي يستخدم السلاح، ونتيجة ذلك فإنها تؤدي إلى إحداث تغييرات في عملية المعلومات الخاصة بالعدو تجعله يتخذ قرارات وفقاً لرغبات المتحكم في النظام، وبالتالي فهو يتشابه مع مصطلح التحكم الانعكاسي الانعكاسية Reflexive Control[3].

1-Franklin D. Kramer, Stuart H. Starr, Larry Wentzeds,cyber power and national security, **Op.Cit**, p 477.

2- الدكتور سيرجي الكسندر وفي كمار كوف Sergei Alexandrovich Markov ولد عام 1958، حصل على الدكتوراه في العلوم السياسية، وأحد الصحفيين والناشطين الاجتماعيين، ويعتبر من العلماء في مجال العلوم السياسية، كما شغل العديد من المناصب سواء الأكاديمية أو الحكومية أو الدولية.

3-Franklin D. Kramer, Stuart H. Starr, Larry Wentz ,eds, Cyberpower and National Security**, Op. Cit**. P 479.

منهج الدراسة:

يعتمد الكاتب في تحليله لاستخدام القوة الإلكترونية في التفاعلات الدولية على الاقتراب الذي طوره فريق عمل تابع لجامعة الدفاع الوطني الأمريكية لدراسة أثر الفضاء الإلكتروني على الأمن القومي، خاصة الأمريكي، **يأخذ في الاعتبار تعظيم الاستفادة من مجالات الفضاء الإلكتروني والحافظ على تفوق وتقدم الولايات المتحدة، وانطلاقاً من ذلك:**

يرى هذا الاقتراب أن مصطلح القوة الإلكترونية يتضمن 4 عناصر يجب أخذها في الحسبان تتمثل في التالي[1]:

1- اعتماد الدول المتزايد على الفضاء الإلكتروني في مجال الأمن القومي والقضايا التجارية والمجتمعية.

2- الأخذ في الاعتبار الدول الأخرى التي تستخدم الفضاء الإلكتروني وباقي الفواعل من غير الدول.

3- الصعوبات والتحديات التي تواجهها الولايات المتحدة في هذا الشأن.

4- التغيرات الاستراتيجية المتوقعة في بيئة الفضاء الإلكتروني.

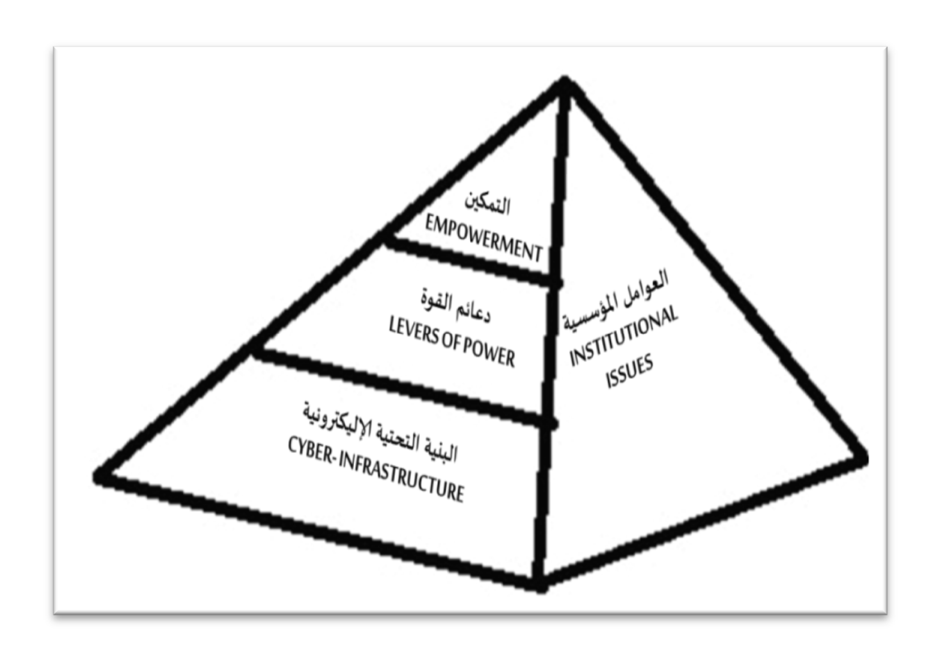
ويأخذ هذا الاقتراب شكلاً هرمياً (شكل رقم 1) وضم ثلاث طبقات أو مستويات على النحو التالي:

1- البنية التحتية الإلكترونية وهي تمثل قاعدة الهرم، وتتمثل في المكونات والأدوات التي تستخدمها هذه البيئة، سواء كانت مكونات مادية Hardware أو برمجية Software، فضلاً عن الاستراتيجيات ونظم الاتصالات والعناصر البشرية.

1-Ibid, 43-44.

2- دعائم القوة Levers of Power، حيث يشهد هذا المستوى تفاعل القوة الإلكترونية الناتجة من المستوى الأول مع الأبعاد الناعمة والصلبة للقوة.

3- يحتل قمة الهرم الكيانات التي من المفترض أن تُمكنهم Empowerment مخرجات المستوى الثاني، وقد تكون هذه الكيانات أفراداً أو شركات أو دولاً أو منظمات أو جماعات إرهابية أو إجرامية(1).



ويفترض هذا الاقتراب أن كل المستويات السابقة تحكمها عوامل مؤسسية وقانونية وضمانات الحريات المدنية. ويؤكد هذا المنهج أنه "إذا كانت الجماعات من غير الدول تمتلك مداخل لبعض أشكال القوة وليست جميعها، فتبقى الدولة وحدها هي القادرة على ممارسة جميع أشكال القوة" بما تمتلكه من موارد وإمكانات مادية

1-Stuart H. Starr, "Toward a Preliminary Theory of Cyberpower", In Franklin D. Kramer, Stuart H. Starr, Larry Wentz,eds, **Cyberpower and National Security**, (Washington D.C: National defense University, May 2009) pp46- 49.

وبشرية وقانونية، وعلى الرغم من ذلك فقد "تظهر بعض العوائق التي تمنع الدولة من ممارسة كافة أشكال القوة كالردع والمعاهدات الدولية التي تلتزم بها الدولة"[1].

وسوف يتم توظيف هذا الاقتراب في تحليل استخدام القوة الإلكترونية في الدراسة على النحو التالي:

أولاً: التعرض للبنية التحتية الإلكترونية الأمريكية وعناصر القوة الإلكترونية المادية والبرمجية Hard Ware And Software، فضلاً عن العقيدة والاستراتيجية ونظم الاتصالات والعناصر البشرية.

ثانياً: تفاعل القوة الإلكترونية مع القوة الناعمة والصلبة في التفاعلات الدولية بين الولايات المتحدة والدول الأخرى.

ثالثاً: القيود التي تفرضها العوامل المؤسسية والقانونية على استخدام القوة الإلكترونية الأمريكية.

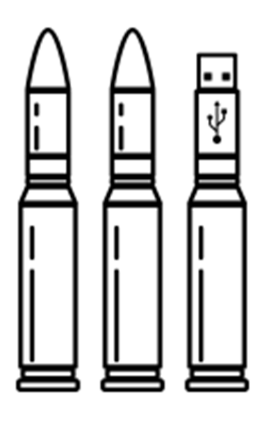
وأخيراً، ينقسم هذ الكتاب إلى ثلاثة فصول بالإضافة إلى المقدمة والخاتمة، فيحلل**الفصل الأول** القوة الإلكترونية وأبعاد التحول في مفهوم القوة، وذلك في ثلاثة مباحث منفصلة، ويتناول **الفصل الثاني** أبعاد القوة الإلكترونية الأمريكية وعناصر حدودها خلال رئاستي بوش وأوباما وذلك في ثلاثة مباحث أيضاً، ويدرس **الفصل الثالث** تطبيقات لاستخدام القوة الإلكترونية الأمريكية في التفاعلات الدولية السياسية والعسكرية والاقتصادية خلال رئاستي بوش وأوباما في ثلاثة مباحث أيضاً.

1-Ibid.

الفصل الأول

القوة الإلكترونية وأبعاد التحول في مفهوم القوة

شهد مفهوم القوة، منذ نهاية الحرب الباردة، جملة من التغيرات لمواكبة التطور الحادث في حقل العلاقات الدولية، خاصة مايتعلق منها بمفهوم الأمن، ويمكن التمييز بين مستويين للتغير الذي طرأ على مفهوم القوة، مستوى خاص بالعناصر المكونة للقوة، والأشكال المختلفة التي تتخذها، ومستوى آخر خاص بالطرف الذي يمتلك القوة، خاصة مع امتلاك فاعلين من غير الدولة بعض مصادر القوة والتأثير في العلاقات الدولية، ومن ثم يسعى هذا الفصل إلى دراسة التغيرات التي أثرت على أشكال القوة، خاصة التكنولوجيا الحديثة لما لها من أثر مهم على تطور ممارسة القوة والنفوذ في العلاقات الدولية وكذلك الوقوف على الفواعل والأطراف التي تمارس هذه القوة، سواء كانت فواعل من الدول أو من غير الدول، ولذلك ينقسم هذا الفصل إلى ثلاثة مباحث، يتناول أولها **الفضاء الإلكتروني وتحولات القوة**، بينما يحلل المبحث الثاني **انتشار القوة والفواعل الدولية في مجال استخدام القوة الإلكترونية**، بينما يدرس الأخير **عناصر القوة الإلكترونية وأبعاد استخدامها في التفاعلات الدولية.**



المبحث الأول:

الفضاء الإلكتروني وتحولات القوة

يسعى هذا المبحث إلى معرفة التحولات التي طرأت على القوة نتيجة التقدم التكنولوجي، خاصة في مجال الإنترنت، والأبعاد الجديدة التي فرضتها عليها التكنولوجيا الحديثة، حيث تُعد القوة من المفاهيم المعقدة، فعلى الرغم من بساطتها الظاهرية من حيث كونها كلمة تتألف من خمسة أحرف، فإنه من الصعوبة تحديد ما هو المقصود بالقوة فعلاً، والجدل حول معنى القوة قديم متجدد، حيث جادل الفيلسوف الفرنسي ميشيل فوكو بأن أساس القوة هو التفاعل، ومن مقولاته الشهيرة: إذا كان يفترض في القوة أنها توجد في الكون بطريقة مركزة أو منتشرة، فإنها لا توجد على هذا النحو. القوة توجد عندما تُستخدم"[1]، في حين جادل ألفن توفلر بأن "المعرفة هي القوة" وأن امتلاك المعرفة هو الأساس لامتلاك الثروة والقوة العسكرية[2].

وقد ساهم العلم والتكنولوجيا في تغيير موازين القوى خلال العصور المختلفة، فانتقلت القوة من إسبانيا والبرتغال القوتين العظميين في أوروبا في القرن الخامس عشر الميلادي، إلى هولندا التي أصبحت القوى العظمي في القرن السابع عشر، واحتلت المرتبة الأولى بفضل تطور قوتها البحرية الضاربة، ولكن اندلاع الحروب بينها وبين انجلترا وفرنسا أضعف من قوة هولندا، وأصبحت بريطانيا وفرنسا من أقوى الدول الأوروبية، وفي منتصف القرن العشرين تغير الميزان الدولي من فرنسا وبريطانيا، إلى الولايات المتحدة الأمريكية والاتحاد السوفييتي، وذلك عقب امتلاك الأسلحة النووية، وتطوير صواريخ عابرة للقارات، وبذلك ساهم العلم والتكنولوجيا في تغيير موازين القوى الدولية، وانتقالها من دول إلى أخرى ومن إقليم إلى آخر.

1- عبدالعزيز العيادي، **ميشيل فوكو.. المعرفة والسلطة**، (المؤسسة الجامعية للدراسات والنشر والتوزيع، الطبعة الأولى، 1994)، ص 44.
2- الفن توفلر، **تحول السلطة**، ترجمة لبنى الريدي، (الهيئة المصرية العامة للكتاب، 1995)، ص 25.

أولاً: ما هي القوة؟

إن تعددت واختلفت تعريفات القوة، فهي إجمالاً يمكن النظر إليها على أنها القدرة على التأثير في الآخرين للحصول منهم على نتائج محددة يسعى الطرف الذي يقوم بعملية التأثير للحصول عليها، كما ربط "هانز مورجنثاو" القوة بفكرة التأثير أو التحكم في المكاسب، وعرّف القوة بأنها القدرة على التأثير في سلوك الآخرين[1]، وقد استفاد عالم الاجتماع "روبرت دال" من أفكار مورجنثاو حول القوة وقدم تعريفاً أكثر وضوحاً للقوة، حيث عرفها بأنها "القدرة على جعل الآخرين يقومون بأشياء متناقضة مع أولوياتهم، ما كانوا يقوموا بها لولا ممارسة تلك القدرة"[2]، كما جادل ستيفن لوكس عام 1974 في كتابه "القوة: رؤية راديكالية" بأن القوة مرتبطة بتحديد الأجندة، للتأثير في سلوك الدول، وبالتالي لا تعني القوة بالضرورة الإكراه[3].

تتعدد أدوات ممارسة القوة في العلاقات الدولية وفقاً لقدرات وإمكانيات ورغبات القوى المشاركة فيه، فقد تكون القوة العسكرية من أهم هذه الأدوات، وقد تكون القوة الاقتصادية والحصار الاقتصادي والمالي، وقد تكون الأداة المعلوماتية من خلال وسائل الاتصال والتكنولوجيا الحديثة والإنترنت، ولما للتكنولوجيا الحديثة من أثر على مفهوم القوة وتحولاتها ظهر مفهوم القوة الإلكترونية Cyber Power.

ومن الأمور المستقرة في العلاقات الدولية أن مصادر قوة الدولة ومكونات نفوذها تتغير، وأن القوة العسكرية وحدها لم تعد تحقق الأهداف المرجوة التي تسعى الدولة لتحقيقها، وأن أشكال القوة متغيرة فمنها القوة الصلبة والتي تتمثل في القدرات

1- Hans J. Morgenthall, **politics Among Nations**, (New York , Altred A. Kreptp ,1948), P 140
2-Joseph S. Nye, **Cyber Power,** (Cambridge: Harvard Kennedy School, Belfer center for Science and International affairs, May 2010), p2.
3- Steven Lukes,**Power: A radical View**, (British sociological association ,1974), p 14.

العسكرية والاقتصادية، وهناك القوة الناعمة والتي تتمثل في العوامل غير المادية كالثقافة والقيم[1].

وإذا كانت الحرب هي الشكل التقليدي لاستخدام القوة، فإن شن الحرب لم يعد يقتصر على استخدام القوة العسكرية فقط، فكما رأي اثنان من جنرالات الحرب الصينيين ليانج وإكسيانج سو في كتابهما "حرب غير مقيدة" فإن أدوات القوة سوف تُستخدم في الحروب وكل المعلومات ستكون منتشرة في كل مكان وستكون أرض المعركة في كل مكان. وبالتالي أصبحت القوة تعني كل شيء تقريباً يسمح بممارسة الضغط النفسي والسياسي الذي هو جوهر القوة من أجل تحقيق غايات محددة[2].

ثانياً: القوة في فكر المدرسة الواقعية:

يعتبر مفهوم القوة من المفاهيم المركزية في فكر المدرسة الواقعية التي ترى أن السياسة الدولية هي عبارة عن صراع من أجل القوة، وأن النظام الدولي يتسم بالفوضوية، وبالتالي تعتمد فيه الدول القومية على قدراتها، فالعالم هو عالم الصراع والحرب وهما أساس العلاقات الدولية ولكل دولة مجموعة من المصالح التي تريد تحقيقها وهي ثلاث مصالح رئيسية مصلحة البقاء، ومصلحة تعظيم القوى العسكرية، ومصلحة تعظيم القوة الاقتصادية وجميع تلك المصالح متشابكة في ارتباط كل واحدة بالأخرى.

تؤكد المدرسة الواقعية في تحليلها لمفهوم القوة على المكون العسكري لفهم وتحليل التفاعلات الدولية، وقد تأسس فكر المدرسة الواقعية على عدة افتراضات من أهمها أن الدولة هي الفاعل الرئيسي المسيطر على العلاقات الدولية، وأنها تتسم بالعقلانية التي تجعلها تحدد مصالحها استجابة لهيكل القوة في النظام الدولي الذي

1-Joseph S. Nye, Soft Power: The Means To Success In World Politics, **Op. cit**., p x.

2- إيمان رجب، لماذا القوة؟، **مجلة السياسة الدولية، ملحق اتجاهات نظرية (القوة: كيف يمكن فهم تحولات القوة في السياسة الدولية؟)**، عدد رقم (188)، (مركز الأهرام للدراسات السياسية والاستراتيجية، أبريل 2012)، ص 3.

يتسم بدوره بالفوضى، مما يفرض على الدول ضرورة الاعتماد على الذات لتحقيق أمنها، وتسعى الدولة لتحقيق الأمن من خلال تسخير كل المصادر المادية لقوتها الفعلية والكامنة، خاصة القوة العسكرية التي تعد من وجهة نظر الواقعية البعد الأهم في قوة الدولة، حيث تتحدد أهمية العناصر المادية الأخرى بالقدر الذي تقوي به البعد العسكري.

وقد استخدام معظم مفكري الواقعية مفهوم القوة بمعنى عناصر قوة الدولة Resources، والتي قد تتسع لتشمل عناصر متعددة، منها عدد السكان، ومعدل الإنفاق العسكري، والموقع الجغرافي، بينما قد تضيق عند البعض الآخر لتقتصر على عنصر مادي واحد.

وقد تطورت هذه النظرة المبسطة للقوة في اتجاهين، عبر عن الاتجاه الأول إسهام روزناو، الذي ميز بين امتلاك القوة، والذي عبر عنه بمصطلح القدرة Capability أي امتلاك عناصر القوة، وبين القدرة على استخدامها لتحقيق أهداف محددة، وهو ما عبر عنه بمصطلح التأثير أو النفوذ Influence فإذا كانت القوة تعرف من جانب المدرسة الواقعية على أنها قدرة الدولة (أ) على السيطرة على أفعال الدولة (ب) حتى تحقق النتائج المطلوبة، فإن امتلاك الدولة لعناصر القوة لا يعد مؤشراً كافياً على القدرة على تغيير سلوك الآخرين، بينما عبر عن الاتجاه الثاني بعض مفكري الواقعية الذين أدركوا ضرورة النظر إلى عناصر قوة الدولة في ضوء علاقات القوى، أي النظر إلى القوة كمسافة Distance بين الدول، حيث تؤثر القدرات القومية في السلوك الخارجي للدولة باعتبارها خصائص ذات طبيعة نسبية، أي عند مقارنتها بالقدرات القوية للدول الآخر التي تتعامل معها، وبالتالي فإن العلاقة بين امتلاك الدولة للقدرات القومية وزيادة قدرتها على التأثير ليست طردية، حيث إن تأثير تلك القدرات يعتمد إلى حد كبير على متغيرات وسيطة مثل عنصر الإدراك سواء بالنسبة لصانع السياسة الخارجية في الدولة أو صانعي السياسة في الدول الأخرى.

وقد أخذ هذا المفهوم الواقعي الضيق للقوة في الاتساع ليشمل عناصر غير مادية، وهو ما ظهر في إطار بعض الكتابات المرتبطة بالواقعية الجديدة التي اعتمدت

بالأساس على المنهجية الاقتصادية، كما ركزت بعض الأدبيات المرتبطة بنظرية الهيمنة على قضية استمرار سيطرة القوة المهيمنة على قمة النظام الدولي بوسائل أقل تكلفة وأكثر قبولاً، وبأدوات بديلة عن الأداة العسكرية، وركزت على مجموعة من الأبعاد المعيارية بحيث يتم الاهتمام بتنشئة النخب في الدولة الهدف، عن طريق تغيير القيم والمعتقدات الجوهرية لهم، بما يؤدي في النهاية إلى تبنيهم سياسيات محددة، وتحديد الأجندة السياسية لهم بما يتفق وتصورات الدولة المهيمنة في النظام، وعلى الرغم من أن هذا النموذج قد ارتكز على مزيج من الأبعاد المادية وغير المادية للقوة، إلا أن أصحابه يرون أنه لا يقلل من أهمية استخدام العناصر المادية كأحد مصادر قوة الدولة المهيمنة.

تعد المدرسة الواقعية من أولى المدارس التي تعاملت مع القوة كمفهوم مركزي لمقولاتها، وترى أنه يمكن تحديد قوة الدولة (أ) عن طريق معرفة المحصلة النهائية للتأثير الذي تمارسه في الدول الأخرى، بهدف امتلاك مزيد من الموارد، كما تتعامل المدرسة الواقعية مع العلاقات الدولية على أنها صراع الهدف منه تعظيم ما تمتلكه الدولة من قوة[1].ويعتبر مفهوم القوة من المفاهيم المركزية في فكر المدرسة الواقعية التي ترى أن السياسة الدولية هي عبارة عن صراع ونزاع من أجل القوة، وأن النظام الدولي يتسم بالفوضوية، وبالتالي تعتمد فيه الدول القومية على قدراتها، فالعالم هو عالم الصراع والحرب، وهما أساس العلاقات الدولية، ولكل دولة مجموعة من المصالح التي تسعى إلى تحقيقها، وهي ثلاث مصالح رئيسية، مصلحة البقاء، ومصلحة تعظيم القوة العسكرية، ومصلحة تعظيم القوة الاقتصادية وجميع تلك المصالح متشابكة كل واحدة بالأخرى[2].

وهناك اتجاه آخر لتعريف القوة، عبرعنه كينيث والتز، حيث وسع مفهوم القوة في المدرسة الواقعية الجديدة ليشمل عناصر أخرى غير عسكرية، وحاول الربط بين قوة الدولة، وامتلاك عناصر مثل المساحة، والموقع الجغرافي، والموارد المادية

1- إسماعيل صبري مقلد، **العلاقات السياسية الدولية: دراسة في الأصول والنظريات**، (القاهرة: المكتبة الأكاديمية، 1984)، ص 19.

2 - James E. Dougherty and Robert L. Pfaltzgraff, Jr., **Contending Theories of International Relations**, (Longman, 2001) pp 63-100.

والطبيعية، والسكان، ودرجة النمو الاقتصادي، والتطور العسكري، والاستقرار السياسي والكفاءة[1].

وقد كان من السهل قديماً تقييم قدرات وإمكانيات الدول، وقياس قوتها، حيث ارتبط تعريف القوة تاريخياً بـ "القوة في الحرب"، واعتبرت عناصر مثل السكان، والأرض، والموارد الطبيعية، والقوة الاقتصادية، والاستقرار السياسي، والقوة العسكرية، هي المكونات الرئيسة لمفهوم القوة، فإذا كان لدى الدولة أسطول قوي وجيش مدرب بشكل جيد، وكذلك قوة ديموغرافية واقتصادية، فمن المحتمل أن تكون قادرة على إجبار أو إكراه، أو حتى رشوة جيرانها، ومن ثم دفعهم إلى الامتثال لأهدافها.

فالقوة الصلبة بهذه الصورة تعني القوة المشتركة السياسية والاقتصادية والعسكرية أي القوة في صورتها الخشنة التي تعني الحرب، والتي تستخدم فيها الجيوش، وهذه القوة تعني الدخول في مزالق خطرة، ونتائجها تكون في منتهى الخطورة على الدولة ذاتها، كما حدث مثلاً في الحرب العالمية الثانية مع اليابان وألمانيا النازية.

لكن عبر القرون، وازدهار التكنولوجيا وتطورها، تغيرت مصادر القوة، فلم تعد تلك المصادر التقليدية التي تميزت بها القوى الدولية التقليدية في قرون ماضية، فعلى سبيل المثال كان عنصر السكان أحد مصادر القوة، وذلك من خلال دفع الضرائب التي تستخدم في التمويل العسكري وتجنيد المواطنين الصالحين في الجيش، وكان عنصراً حاسماً في المعارك الحربية، بينما نجد حالياً أن امتلاك التكنولوجيا العسكرية الحديثة والأسلحة غير التقليدية، أصبحت عناصر حاسمة في المعارك الحربية.

1- Keneeth N. Waltz, Man, **The State & War**, (Athearetical Analysis N .Y :Colombia Unversity Press , 1959), pp . 159 – 160.

ثالثاً: القوة في فكر المدرسة الليبرالية:

قامت المدرسة الليبرالية على رفض افتراضات المدرسة الواقعية، فالدولة ليست محدداً رئيسياً للسياسة الدولية، وبررت ذلك بأن الساحة الدولية قد شهدت تنامياً في أدوار فاعلين جدد، لعبوا دوراً في التأثير في سلوك الدولة، ولا يمكن تجاهله، كما بررت موقفها بتزايد أهمية دور العلاقات العابرة للقوميات، وفي التأثير في السياسة الخارجية للدولة بطريق مباشر أو غير مباشر، من خلال فرضها قيوداً على سلوك الدول، نتيجة الاعتماد المتبادل، أو من خلال تغيير توجهات سياستها الداخلية[1].

وبتطور السياسة الدولية، وارتفاع تكاليف استخدام الأداة العسكرية، حتى بالنسبة للدولة المهيمنة على قمة النظام الدولي، طرح جوزيف ناي – أحد مفكري المدرسة الليبرالية –، مفهوم القوة الناعمة، كشكل آخر للقوة، وقد عرف ناي القوة الناعمة بأنها: القدرة على جعل الآخرين يريدون النتائج التي تريدها بالاعتماد على قوة الجاذبية وإقناع الآخرين وبدون إرغامهم على فعل ذلك[2].

كما يرى جوزيف ناي: أنه "وإن أمكن الوصول للأهداف من خلال القوى الصلبة، إلا أن ذلك قد يشكل خطراً على الأهداف والتطلعات الاقتصادية والسياسية للدولة". وبالتالي يجب أخذ القوة الناعمة في الاعتبار، وقد عرف جوزيف ناي في تسعينيات القرن المنصرم مفهوم القوة الناعمة بأنه القدرة على جذب الآخرين والتأثير فيهم من خلال القيم والمعتقدات، وليس من خلال التهديد أو استعمال القوة العسكرية أو الاقتصادية[3]، حيث تشكل القوة الناعمة أحد أشكال القوة التي تستخدمها الدول في سياستها الخارجية وتشكل إطاراً عاماً من الأنماط والسلوكيات الثقافية، والتي تسعى الدول لنشرها على المستوى الخارجي من أجل تحقيق أهدافها، وبالتالي فإذا كانت القوة الصلبة تنبع أساساً من القدرات العسكرية

1- د.سعاد محمود أبو ليلة، **مرجع سبق ذكره**، ص ص 14.

2- Joseph S. Nye, **Soft Power: The means to success in world politics,** (New York: Public Affairs, 2004), pp 1-5.

3- Joseph S. Nye, The Decline of America's Soft Power, **Foreign Affairs**, May/ June 2004.

والاقتصادية، فإن القوة الناعمة تتأتى من جاذبية النموذج، وما يمتلكه من قدرة التأثير والإغراء للنخب والجمهور على السواء.

وارتباطاً بالسياق السابق وضع ناي نموذجاً يوظف فيه القوة الإلكترونية كأداة للتفاعلات الدولية بجانب كل من القوتين الصلبة والناعمة.

من ناحية أخرى أعادت النظرية الليبرالية تعريف القوة، حيث ترى أن القوة تتمثل ليس فقط في القوة العسكرية، ولكن أيضاً في القوة الاقتصادية، ويرى جوزيف ناي أن هذين النوعين يمثلان القوة الصلبة، ولكن هناك بعداً آخر من القوة يمكن للدولة من خلاله تحقيق أهدافها يتمثل في جاذبية النموذج والقيم والقدرة على الإقناع، إذ بإمكان دولة ما أن تنال النتائج التي تسعى لتحقيقها، وذلك لأن الدول الأخرى تريد أن تتبعها وتعجب بقيمها وتتشبه بها وتطمح للوصول إلى مستواها، وهو ما أطلق عليه ناي اسم "القوة الناعمة"[1].

وقد ارتبط الحديث عن القوة الناعمة كأحد أشكال القوة بمحاولات جوزيف ناي معالجة التحليل الضيق لمفهوم القوة الذي قدمته المدرسة الواقعية والذي كان يركز على القوة العسكرية، حيث ميَّز ناي بين ثلاثة أنماط من القوة الناعمة هي الجاذبية Attraction ويشير إلى جذب الانتباه إما بطريقة سلبية أو إيجابية، والنمط الثاني هو الإقناع Persuasion ويستخدم للتأثير في معتقدات الآخرين وردود أفعالهم دون التهديد باللجوء إلى القوة، وينصرف النمط الثالث إلى وضع جدول الأعمال أو ما يطلق عليه Agenda Setting وتحديد أولويات الدول الأخرى بما يخدم أو يتفق مع أولويات الدولة التي تمارس القوة الناعمة[2].

قام جوزيف ناي بتطوير أفكار لوكس، وقدم مفهوماً، ربما يكون أكثر تعقيداً للقوة، حيث اهتم بعناصرها غير المادية مثل الثقافة والقيم، من خلال مفهوم القوة

1- Ibid, 416-447.

2- ريهام مقبل، "مركبالقوة: عناصروأشكالالقوةفيالعلاقاتالدولية"،**مجلة السياسة الدولية، ملحق اتجاهات نظرية (القوة: كيف يمكن فهم تحولات القوة في السياسة الدولية؟)**، عدد رقم 188، (مركز الأهرام للدراسات السياسية والاستراتيجية، أبريل 2012)، ص 7.

الناعمة. وعرفها بأنها "قدرة الدولة على الحصول على ما تريده بالاعتماد على الجاذبية بدلاً من الإكراه[1]". وتعبر **القوة الناعمة** عن الوجه الثاني للقوة، حيث تتمكن دولة ما من الحصول على النتائج التي تريدها لأن الدول الأخرى معجبة بنموذجها، وتحاول أن تتبعه، وليس لأنه يتم إكراهها على ذلك. ومع ثورة المعلومات، أُضيف عنصر جديد لقوة الدولة، حيث أصبح من عناصر قوة الدولة امتلاك التكنولوجيا والمعلومات، والقدرة على إنتاج التكنولوجيا المتطورة عن طريق الاختراع، والإبداع، ونشر الإبداع أيضاً[2].

ويشير جوزيف ناي إلى أن البعض يفكر في القوة بصورة خاطئة، ويرى أن تعريف القوة بأنها القدرة على جعل الآخرين يفعلون ما لا يريدون، هو في ظاهره قد يكون غير دقيق، خاصة إذا كان الأمر يتعلق بتغيير سلوكيات الآخرين، ويجادل بأنه يجب معرفة أولويات الآخرين حتى نستطيع قياس التغير في السلوك نتيجة القوة، ويدلل على ذلك بأن الديكتاتور الذي يسعى لإعدام معارض سياسي بريء قد يفقد معنى قوته إذا كان ذلك البريء يسعى بالفعل للاستشهاد، كما أنه مخطئ من يظن أن صياح الديك هو الذي يجعل الشمس تشرق[3].

ويؤكد ناي أنه يمكن الحصول على النتائج المرجوة والتأثير في سلوكيات الفاعلين من دون اللجوء إلى القوة، وهو ما يدفع البعض إلى تنفيذ أوامر البابا، ليس خوفاً من عقاب، ولكن إيماناً بسلطته الأخلاقية والروحية، وبالمنطق نفسه نجد أن هناك مؤيدين لزعيم القاعدة – السابق – أسامة بن لادن من المسلمين المتشددين، ليس خوفاً من عقاب أو تهديدات، ولكن إيماناً بشرعية أهدافه[4].

عرف جوزيف ناي في تسعينيات القرن المنصرم مفهوم القوة الناعمة بأنه القدرة على جذب الآخرين والتأثير فيهم من خلال القيم والمعتقدات، وليس من خلال التهديد أو استعمال القوة العسكرية أو الاقتصادية[5]، أي القدرة على الحصول على

1- Joseph S. Nye, Soft Power: The Means To Success In World Politics, **Op. Cit**., p 2.

2- ريهام مقبل، **مركب القوة: عناصر وأشكال القوة في العلاقات الدولية**، مرجع سبق ذكره ص ص 6-10.

3- Joseph S. Nye, Soft Power: The Means To Success In World Politics, **Op. Cit**., p 2.

4-Ibid.

5- Joseph S. Nye, The Decline of America's Soft Power, **Foreign Affairs**, May/ June 2004.

النتائج المرجوة من خلال الجاذبية وليس الإكراه، وذلك بالاعتماد على جاذبية ثقافة الدولة، وأفكارها السياسية، وسياساتها[1].

ومن ثم تشكل القوة الناعمة أحد أشكال القوة التي تستخدمها الدول في سياستها الخارجية وتشكل إطاراً عاماً من الأنماط والسلوكيات الثقافية التي تسعى من خلالها الدول لنشرها على المستوى الخارجي من أجل تحقيق أهدافها، وذلك عبر مجتمع المعلومات مثل: نشر الأفكار والمعلومات، ودعم قنوات البث الإذاعي والإرسال التلفزيوني، وترويج سلع ثقافية وخدمات وبرامج معلوماتية يكون هدفها دعم المعارضة للنظم القائمة[2]، أو السياسات الخاصة بالمنظمات الدولية وتقديم المعونات الاقتصادية وتنفيذ مشاريع اقتصادية وتجارية، أي باختصار تحقيق هدف تم الاتفاق عليه وعلى إنجازه بأساليب فكرية وإقناعيه من دون اللجوء للعنف.

ويأتي في سياق القوة الناعمة دور الإعلام في عصر العولمة أو "إعلام العولمة" والذي يعني تعاظم قدرة وسائل الإعلام والمعلومات على تجاوز الحدود السياسية والثقافية بين الدول والمجتمعات بفضل وسائل التكنولوجيا الحديثة[3]، حيث أصبح امتلاك القدرة على المساهمة في الثورة المعلوماتية أساس القوة في العلاقات الدولية، والوسيلة التي تتمكن خلالها دولة أو بعض الدول من بسط نفوذها والهيمنة على الدول الأخرى في النظام الدولي الجديد، حيث تطور مفهوم القوة من القوة العسكرية ثم القوة الاقتصادية إلى قوة المعلومات ومدى قدرة الذكاء والنشاط البشري على توظيفها واستخدامها[4].

1-Joseph S. Nye, Soft Power: The Means To Success In World Politics, **Op. cit**., p x.

2- يحيى اليحياوي، **عن قوة أمريكا "الناعمة"**، يونيو 2004، 12 مايو 2013، دراسة منشورة على :
http://www.elyahyaoui.org/softpower.htm

3- أدهم عدنان طبيل، الإعلام الحديث في ظل العولمة، **صوت الوطن**، دراسة منشورة بتاريخ 25 مايو 2007، تم الاطلاع ليها بتاريخ 30 يوليو 2013:
http://pulpit.alwatanvoice.com/articles/2007/05/25/89911.html

4- إسراء أحمد وشريف رشدي، **الواقع الافتراضي والتغيير السياسي في العالم، دراسة في ثورات الوطن العربي،** (مركز المعلومات ودعم اتخاذ القرار، يونيو 2011)، ص 43.

يؤكد ناي في كتابه القوة الناعمة أن مصادر هذه القوة الناعمة لدى الدول ثلاث:

- **الثقافة**: والتي تكمن في جاذبيتها للآخرين.

- **القيم السياسية**: والتي تترسخ في النخبة الحاكمة والمحكومة.

- **السياسة الخارجية**: والتي ينظر إليها مختلف الفواعل الدولية على أنها شرعية وأخلاقية.

ويرى ناي أن الثقافة هي نسق من القيم والممارسات التي تخلق معنى للمجتمع، فإذا تبنت الدولة في سياساتها ثقافات وقيم عالمية يشارك الآخرون فيها وليست قيماً ضيقة تعبر عن ثقافة خاصة، فإن من شأن ذلك حصول هذه الدولة على النتائج التي ترجوها، كما أن القيم التي تعتقد فيها الدولة كالديمقراطية، والسياسات التي تتبعها كحقوق الإنسان، تضفي مزيداً من الشرعية على أهداف الدولة بما يساعد في تحقيقها[1].

ولكن هذا لا يعني إغفال دور القوة الصلبة، فكلاهما وجهان لعملة واحدة، ولا تغني إحداهما عن الأخرى، فكلتاهما تؤثران في السلوك وتسعى لدفع الآخرين للقيام بأفعال لم يكن ليقوموا بها، ولكنهما تختلفان في أدوات ممارسة هذه القوة، فبينما تعتمد الأولى على الإكراه تعتمد الثانية على الجاذبية، ويختلفان أيضاً في مصادر القوة، فبينما تعتمد الأولى على القوة العسكرية والاقتصادية، تعتمد الثانية على القيم والثقافات والمؤسسات[2].

وحسب ناي، فإن هناك خمسة تحولات دولية ساهمت في تراجع دور القوة الصلبة أو على الأقل قلّلت من فاعليتها، تمثلت في **الاعتماد الاقتصادي المتبادل بين الدول** بما ساهم في الحد من الاستخدام الصلب للقوة لمخاطرها على النمو الاقتصادي، فضلاً عن **ظهور فواعل أخرى غير الدول** أصبحت قادرة على ممارسة

1- Joseph S. Nye, Soft Power: The Means To Success In World Politics**, Op. cit**., pp 10-14.
2-Ibid, pp 7-9.

أنواع القوة مثل الفاعلين غير القوميين، وكذلك الشركات متعددة الجنسية، والمنظمات الدولية سواء الحكومية أو غير الحكومية، والجماعات الإرهابية، بالإضافة إلى **انبعاث النزعات القومية** وهو ما صعّب عملية استخدام القوة، فعلىسبيل المثال، كانت بعض المواقع العسكرية الصغيرة قادرة على إدارة إمبراطورية مثل الإمبراطورية البريطانية، لكن في الوقت الحاضر، فإن الولايات المتحدة، على سبيل المثال، وجدت أنه من الصعب إخضاع العشائر الصومالية أو تهدئة الوضع في العراق،حتى مع زيادة عدد قواتها، وكذلك ساهم **انتشار التكنولوجيا**، خاصة في مجال تطوير الأسلحة النووية، في تعادل قوة الأطراف في أرض المعركة، وأخيراً **التغير الحادث في القضايا السياسية** وظهور قضايا تعجز القوة الصلبة عن حلها، مثل الفقر والتلوث وانتشار الأوبئة والجريمة المنظمة والتغيرات المناخية، كما أن استخدام القوة العسكرية أصبح مكلفاً جداً مقارنة بما كان في القرون الماضية[1].

فحينما تبدو السياسة الأمريكية مقبولة ومشروعة في أعين الآخرين، على ما يقول ناي، "يتعاظم دور القوة الناعمة أكثر، وبموازاة ذلك، تتراجع الحاجة إلى استخدام القوة التقليدية. وعلى العكس من ذلك، فكلما تضخم استخدام القوة الإكراهية، وضعفت شرعية مثل هذا الاستخدام، يتضاءل معها النفوذ الثقافي والسياسي والتجاري، وكل ما يدخل ضمن دائرة القوة الناعمة"[2].

وبالتالي، فإذا كانت القوة الصلبة تنبع أساساً من القدرات العسكرية والاقتصادية، فإن القوة الناعمة تتأتى من جاذبية النموذج، وما يمتلكه من قدرة التأثير والإغراء للنخب والجمهور على السواء. فالقوة الناعمة كما يرى ناي هي قوة جذب، وتتضح في تعدد الوسائل التي يمكن اللجوء إليها للحصول على النتائج المرجوة دون اللجوء إلى استخدام العصا أو الجزرة.

1- **القوة الناعمة الأمريكية آفاقها وتحدياتها،** (دراسة صادرة عن مركز الصحوة للدراسات، بتاريخ 13 نوفمبر 2012) تم الاطلاع عليها بتاريخ 30 يوليو 2013، http://www.essahwa.com/?p=131

2- رفيق عبدالسلام، **الولايات المتحدة الأمريكية بين القوة الصلبة والقوة الناعمة،** (مركز الجزيرة للدراسات، الدوحة، 2008) ص 88.

رابعاً: التحولات في مفهوم القوة تحت تأثير الفضاء الإلكتروني:

بفضل ثورة المعلومات، ومع ظهور الإنترنت ومواقع الويب أصبح الفضاء الإلكتروني أحد العناصر الرئيسية التي تؤثر في النظام الدولي بما يحمل من أدوات تكنولوجيا تلعب دوراًمهماً في عملية التعبئة والحشد في العالم، فضلاً عن التأثير في القيم السياسية وأشكال القوة المختلفة سواء كانت صلبة أو ناعمة.

ويعتبر الفضاء الإلكتروني بيئة مصنوعة وحديثة، حيث يستجيب للتغيرات بصورة سريعة أكبر من البيئات الطبيعية الأخرى، وذلك لاعتماده على التكنولوجيا الحديثة واستجابته السريعة للتطورات التكنولوجية، فإذا كان من الصعب السيطرة أو التحكم أو التنقل بين الإقليم البري أو البحري أو الجوي أو الفضاء الخارجي، فإنه يمكن التجول بلا حدود في الفضاء الإلكتروني بمجرد ضغطة على مفتاح التشغيل الخاص بالكمبيوتر، فهو يتميز بسهولة الاستخدام ورخص التكلفة وسهولة الحصول على المعلومات وتوافرها، فضلاً عن إمكانية التخفي وعدم الظهور بالشخصية الحقيقية الملموسة على أرض الواقع، وقد شجع كل ذلك على تعدد الفاعلين المستخدمين للفضاء الإلكتروني، فشمل بذلك أفراداً وجماعات ودولاً ومنظمات دولية وشركات، كما تعددت استخداماته فأصبح له استخدامات تجارية ومالية واقتصادية وعسكرية واجتماعية وعلمية ومعلوماتية، فإذا كان من الصعب تحريك أسطول دولة معينة في المحيط أو الإقليم البحري للقيام بمهمة معينة، فإنه من اليسير جداً إرسال جيش جرار من الفيروسات وبرامج الكمبيوتر التي تستطيع القيام بعمليات معلوماتية على قدر عال من الأهمية.

وهناك ثلاثة عناصر أساسية أفرزتها ثورة المعلومات هي: المعلومة Information، والفضاء الإلكتروني Cyber Space، والطابع الإلكتروني Digital، وتعتبر كلمة Cyber مقتبسة من علم Cybernetics وهو عبارة عن نظرية الاتصالات والتحكم المنظم في التغذية العكسية التي تعتمد عليها دراسات الاتصالات والتحكم في الحياة وفي الآليات التي صنعها الإنسان، أي علم دراسة الاتصالات والتحكم الآلي في النظم العصبية للكائنات الحية ومحاكاة الآلات لها، وتستخدم كلمة

Cyber مرتبطة بكلمة Space، لتعبر عن الفضاء الإلكتروني لتضم كل الاتصالات والشبكات وقواعد المعلومات والبيانات ومصادر المعلومات[1].

ويختلف الفضاء الإلكتروني عن الفضاء الخارجي في أن الفضاء الإلكتروني يعمل وفق قوانين فيزيائية مختلفة عن قوانين الفضاء الخارجي، فمثلاً لا تزن المعلومات شيئاً ولا تمتلك كتلة مادية وبإمكان المعلومات أن تظهر للوجود وتختفي منه ويتم تعديل وتبادل المعلومات خلال نظم مرتبطة بالبنية التحتية، ويتطلب الفضاء الإلكتروني وجود هيكل مادي من أجهزة الكمبيوتر وخطوط الاتصالات، ومن ثم فإن ما يعمل داخل هذه الأجهزة يمثل نمطاً من القوة والسيطرة، وتصبح القيمة الحقيقية للفضاء الإلكتروني هي الاستفادة من كم المعلومات الموجودة داخله والمساهمة في التحكم بها في إطار وشكل إلكتروني.

ويعد الفضاء الإلكتروني مجالاً عاماً وسوقاً مفتوحة ويدلل على وجود شبكة من التواصل والعلاقات بين من يستخدمونه ويتفاعلون معه مع انتقال كافة مجالات الحياة من إعلام وصحة وتعليم وحكومة ومواطنة واقتصاد وسياسة إلى الفضاء الإلكتروني فيما يشبه بالحياة الأخرى، وإلى جانب ذلك أصبح الفضاء الإلكتروني وسيطاً ووسيلة في الوقت نفسه لشن الهجوم وتنفيذ الأعمال العدائية بين الخصوم كغيره من المجالات كالجو أو الفضاء أو البحر، فهو بمنزلة وسيط جديد للصراع، ويحوي الفضاء الإلكتروني كماً هائلاً ومتسعاً عبر الشبكات ونظم المعلومات والاتصالات تربطه مع الفضاء الخارجي والأقمار الصناعية، وعلى الرغم من درجة التشابه بينه وبين الفضاء الخارجي إلا أنه يختلف في أن الفضاء الإلكتروني تم بناؤه من قبل الإنسان ولم يوجد في الطبيعة[2].

وتستخدم الدول الفضاء الإلكتروني لاعتبارات الأمن والقوة العسكرية بشكل جعل العديد من الدول تدخل الفضاء الإلكتروني ضمن حساباتها الاستراتيجية وأمنها القومي، إلى جانب دور الفضاء الإلكتروني في تحقيق الرفاهية الاقتصادية

1- عادل عبدالصادق، **الإرهاب الإلكتروني: القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة**، (القاهرة، مركز الأهرام للدراسات السياسية والاستراتيجية، 2009)، ص ص 30-40.
2- عادل عبدالصادق، **المرجع السابق**، ص ص 35-40.

والحصول على موارد الثورة والسلطة وتحقيق التفوق السياسي، وتعظيم معرفتها وسباقها العلمي والبحثي والقدرة أيضاً على تحقيق السلم والأمن والتفاهم الدولي من خلال دور الفضاء الإلكتروني كأداة اتصال ووسيلة إعلام دولية.

وتتضح العلاقة بين الفضاء الإلكتروني والأمن الدولي، حيث يوجد المحتوى المعلوماتي العسكري والأمني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي في الفضاء الإلكتروني، خاصة مع التوسع في تبني الحكومات الإلكترونية من جانب العديد من الدول واتساع نطاق مستخدمي وسائل الاتصال وتكنولوجيا المعلومات في العالم، حيث تصبح قواعد البيانات القومية في حالة انكشاف خارجي، وهذا ما يعرضها لخطر هجمات الفضاء الإلكتروني إلى جانب الدعاية والمعلومات المضللة ونشر الشائعات أو الدعوة لأعمال تحريض أو دعم المعارضة الداخلية للنظام الحاكم.

خامساً: القوة الإلكترونية Cyber Power:

ولما للتكنولوجيا الحديثة من أثر على مفهوم القوة وتحولاتها ظهر مفهوم القوة الإلكترونية Cyber Power، حيث يعرفها جوزيف ناي بأنها "القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء الإلكتروني، أي أنها القدرة على استخدام الفضاء الإلكتروني لخلق مزايا، والتأثير في الأحداث المتعلقة بالبيئات الواقعية الأخرى وذلك عبر أدوات إلكترونية[1]". ويعرفها دانيال كويل Daniel T. Kuehl بأنها "القدرة على استخدام الإنترنت لخلق مزايا والتأثير على الأحداث في البيئات التشغيلية كافة من خلال أدوات القوة[2]".

يرى جوزيف ناي أن القوة الإلكترونية مرتبطة بامتلاك المعرفة التكنولوجية، والقدرة على استخدامها. وهي تعني القدرة على استخدام الفضاء الإلكتروني في خلق مميزات والتأثير في الأحداث التي تجري عبر البيئات التشغيلية Operational Environments وعبر أشكال وأدوات القوة المختلفة، سواء كانت عسكرية أو اقتصادية أو دبلوماسية أو معلوماتية[3]، وقد حدد ناي ثلاثة أنواع من الفاعلين الذين يمتلكون القوة الإلكترونية، يتمثل النوع الأول في **الدولة** والنوع الثاني في **الفاعلين من غير الدول** والنوع الثالث هم **الأفراد**، وقد حدد ناي أنماطاً لاستخدام موارد القوة الافتراضية وميز بين الاستخدام الناعم لها والاستخدام الصلب.

ويجادل جوزيف ناي بأن مفهوم القوة الإلكترونية يشير إلى "مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الإلكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل"[4].

1-Joseph S. Nye, Cyber Power **Op Cit**. p4.
2- Daniel T. Kuehl, "**From Cyber Space to Cyber Power: Defining the problems**", in Franklin D. Krammer, Stuart Starr, and Larry K. Wentz. Eds, **cyber power and national security**, (Washington, D.C: National defense up, 2009), p 16.
3-Franklin D. Kramer, Stuart H. Starr, Larry Wentz,eds, **Op.Cit**, p 48.
4-Joseph S. Nye, Cyber Power, **Op. Cit,** P3.

وتتعدد أدوات ممارسة القوة في العلاقات الدولية وفقاً لقدرات وإمكانيات ورغبات القوى المشاركة فيه، فقد تكون القوة العسكرية من أهم هذه الأدوات، وقد تكون القوة الاقتصادية والحصار الاقتصادي والمالي العامل الرئيسي للسيطرة على الخصم وممارسة القوة عليه، وقد تكون الأداة المعلوماتية من خلال وسائل الاتصال والتكنولوجيا الحديثة والإنترنت هي العامل الرئيسي لحسم صراع بين دولتين.

إلا أن ممارسة القوة والنفوذ قد تطورت بشكل هائل نتيجة للتطور الكبير في المعلومات مما جعل هذهِ المعلومات هي الهدف الأساسي الذي تسعى الدول للحصول عليه، هذه المعلومة هي التي مكنت الدول من إنتاج السلاح النووي، وظل هذا التطور مستمراً، حيث اعتمدت كل مرحلة من مراحل التطور الإنساني على سلطة أو قوة من طبيعة معينة تتناسب مع متطلبات هذه المرحلة، ولقد أثرت هذه السلطة أو القوة بصورة مباشرة أو غير مباشرة في أدوات الصراع بين المجتمعات وآلياتها، وأفرزت مفردات ومكونات تكاملت معاً لتنتج نظاماً دولياً سيطرت مفاهيمه بعض الوقت أو كل الوقت، وفي هذا الإطار تميز عصرنا الحالي بظاهرة الثورة العلمية والتكنولوجية ولقد أزاحت وحيدت التكنولوجيا الكثير من عناصر القوة عن مواقعها التي تربعت عليها فترة طويلة، مما عرض المفهوم التقليدي للقوة إلى انتقادات، وأفصح عن محتوى جديد للقوة فلم يعد ما في يد الدولة من قدرات عسكرية أو ما تمتلكه من أموال وثروات، كافية لبلورة دورها كقوة مؤثرة وفاعلة[1].

وأصبحت القوة الإلكترونية حقيقة أساسية في العالم بكل مظاهرها المتنوعة وبما عمل على دعم ومساندة العمليات الحربية والقوة الاقتصادية والسياسية ودور ثورة المعلومات والمعرفة في بروز مجتمع المعلومات الدولي والاقتصاد الإلكتروني الجديد الذي أثر على طبيعة النظام الدولي فيما يتعلق بالتقسيم الدولي للعمل، وهو الذي يحدد آفاق النمو أمام مختلف البلاد، ويعمل أيضاً على توزيع الموارد الاقتصادية ومستويات النمو الاقتصادي، وأنماط التفاعل بين القوى الاقتصادية الدولية، والتأثير على القوة السياسية بالتأثير على عمليات صنع القرار في النظام الدولي.

1- عادل عبدالصادق، الإرهاب الإلكتروني: القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، **مرجع سبق ذكره**، ص ص 50- 58.

ويتضمن مفهوم القوة الإلكترونية تغطية كافة القضايا التي تتعلق بالتفاعلات الدولية والتي تشمل القضايا العسكرية والاقتصادية والسياسية والثقافية والإعلامية وغيرها، وتختلف عن مسمى الحرب الإلكترونية التي تقتصر على التطبيقات العسكرية للفضاء الإلكتروني، وتتم الإشارة إليه بالهجوم الإلكتروني. وإذا كانت ثورة المعلومات لها تأثير على تطوير الجوانب العسكرية للدول، فإن لذلك أبعاداً سياسية واجتماعية، حيث ازدادت القدرات التدميرية للأسلحة، وهنا يثور تساؤل جدلي حول الدور الذي تلعبه التكنولوجيا في الحياة البشرية، فإذا كان لها مميزات تخدم الجنس البشري، فإن لها عيوباً تفضي إلى القضاء عليه، ويثور تساؤل آخر حول دور التكنولوجيا في التأثير على القوميات الوطنية والثقافات الخاصة، والتي أصبحت عرضة للتأثير والتأثر بفضل ثورة الاتصالات وتكنولوجيا المعلومات، حيث أصبحت السيطرة الثقافية لمن يمتلك التكنولوجيا ويستطيع أن يوظفها.

الخلاصة:

ساهم التطور التكنولوجي في تحول أشكال القوة عبر العصور المختلفة، وساهمت ثورة المعلومات في ظهور شكل جديد لها، هو القوة الإلكترونية، تمثل المعلومة ركيزة أساسية فيها، وتتطلب ممارستها امتلاك المعرفة التكنولوجية، حتى تستطيع الدولة أن توظفها بكفاءة في تحقيق أهدافها الخارجية والداخلية، هذا الشكل الجديد من القوة، له استخدامات صلبة وناعمة في الوقت نفسه، ومن ثم فهو ليس فرعاً مستقبلاً بذاته، بل يصلح أن يندرج تحت نوعي القوة التقليديين، الصلبة والناعمة.

المبحث الثاني

انتشار القوة والفواعل الدولية في مجال استخدام القوة الإلكترونية

أفرزت الثورة المعلوماتية القوة الإلكترونية كشكل جديد من أشكال القوة، وهذه القوة كان لها تأثير في علاقات القوة على مستوى السياسة الدولية، فمن ناحية أدت إلى توزيع القوة بين عدد أكبر من الفاعلين مما جعل قدرة الدولة على السيطرة على هذا الميدان موضع شك، مقارنة بالمجالات الأخرى للقوة. ومن ناحية أخرى جعلت القوة الإلكترونية الفاعلين الأصغر في السياسة الدولية لديهم قدرة أكبر على ممارسة كل من القوة الصلبة والقوة الناعمة عبر الفضاء الإلكتروني، وهو ما يعني تغيراً في علاقات القوى في السياسة الدولية، ويسعى هذا المبحث لتحليل المقصود بانتشار القوة في السياسة الدولية والفواعل الدولية في مجال استخدام القوة الإلكترونية بما يمكننا من الوقوف على طبيعة علاقات القوى في مجال الفضاء الإلكتروني وحدود قدرة الدولة على السيطرة على هذه الميدان.

أولاً: المقصود بانتشار القوة:

يعد جوزيف ناي أبرز المستخدمين لمفهوم انتشار القوة ويرى أن هذه الظاهرة تفرض تحديات جديدة على الدول، حيث يعرفها بأنها: "تزايد القضايا ومجالات التأثير والتفاعل الواقعة خارج نطاق السيطرة الكلية للدولة بما فيها الدول الأكثر قوة مع ظهور فاعلين جدد يتمتعون بصور جديدة من القوة"[1]، أي أنها تعني مشاركة فواعل من غير الدول في مصادر القوة التي كانت حكراً على الفواعل من الدول.

1-Joseph S.Nye,Cyber Power, **Op. Cit**, P13.

فإذا كان انتقال القوة ومراكز السيطرة الدولية من دولة إلى أخرى هو أمر مألوف في التفاعلات الدولية عبر العصور، ويمكن ملاحظته في ظهور مراكز دولية تزاحم الولايات المتحدة الأمريكية، مثل الصين والاتحاد الأوروبي، فإن انتشار القوة ظاهرة حديثة، ارتبطت بتعاظم دور الفاعلين من غير الدول، وذلك لأن المعلومة لم تعد حكراً على الدول، فالقطاع الخاص يساهم بنسبة كبيرة في امتلاك وإدارة التكنولوجيا الحديثة ووسائل الاتصالات والمعلومات، ففي السبعينيات كانت إمكانية الحصول على صورة للكرة الأرضية حكراً على الولايات المتحدة الأمريكية والاتحاد السوفييتي، لما تمتلكان من تكنولوجيا تمكنهما من الحصول على ذلك، أما الآن ونتيجة للتقدم التكنولوجي فيمكن لأي فرد أن يحصل على صورة للكرة الأرضية وبأبعاد وفقاً لاحتياجاته من خلال برنامج Google Earth، واذا كانت أنظمة تحديد المواقع الجغرافية حكراً على الجيوش، فإنها حالياً في يد كل فرد عبر أجهزة التليفون المحمول، وتراجعت سيادة الدولة لأول مرة منذ صلح وستيفاليا 1648 الذي أسس لنظام دولي قائم على سيادة الدول القومية، بل يجادل بعض الكاتبين بأن ثورة المعلومات سوف تعمل على تسطيح الهياكل البيروقراطية الدولية، وتعمل على خلق شبكة أفقية من العلاقات بين الفواعل من الدول ومن غير الدول.

ساعد الفضاء الإلكتروني على انتشار القوى بين مختلف الفاعلين، وأعطى مساحة متزايدة للفواعل من غير الدول للتأثير في التفاعلات الدولية، وكان نتيجة لهذا الانتشار أن زادت المخاطر والتهديدات التي تواجهها الدول عبر الفضاء الإلكتروني، وأصبح من الضروري امتلاك مصادر التكنولوجيا الحديثة التي تمكن الدول من مواجهة هذه المخاطر، بل وامتلاك الأسلحة الإلكترونية التي يتم استخدامها.

ثانياً: مستويات انتشار القوة:

يشير مفهوم انتشار القوة إلى بعدين من الانتشار، هما البعد الداخلي والبعد الخارجي، فيشير الحديث عن انتشار القوة داخل الدولة - أي بمعنى السلطة السياسية Authority - إلى زيادة المشاركة في العملية السياسية وفي عملية صنع القرار، سواء من خلال صياغة القواعد الحاكمة لها أو من خلال التأثير في العملية ذاتها[1]، أما البعد الثاني وهو البعد الخارجي لانتشار القوة فيشير إلى انتقال القوة من التركز في الفاعل الأقوى أو مجموعة من الفاعلين الأكثر قوة في الإقليم أو العالم إلى فاعلين آخرين سواء كانوا من الدول أو من غير الدول[2].

وارتباطاً بذلك يمكن التمييز بين مستويين لانتشار القوة، المستوى الأول ويقصد به السلطة التي تتمتع بها الدولة في مواجهة المواطنين، والمستوى الثاني ويقصد به القوة التي تتمتع بها الدولة في مواجهة الدول الأخرى، وعملياً فهناك تداخل بين المستويين، فمن ناحية لا ينتج تراجع دور الدولة في الداخل فقط عن تزايد دور الفاعلين المحليين الآخرين داخلها، وإنما ينتج أيضاً عن انتشار القوة بين الفاعلين الخارجين، سواء كانوا من الدول أو من غيرها، وما يترتب على ذلك من تزايد دورهم في المجالات الداخلية المحجوزة تقليدياً للدولة. ومن ناحية أخرى يمتد تأثر الفاعلين المحليين من غير الدول إلى الخارج بما يسهم في إنهاء احتكار الدولة لدور الفاعل الوحيد في العلاقات الدولية[3].

وفي السياق ذاته خاصة ما يتعلق بالبعد الخارجي لانتشار القوة، هناك اتجاه يبرز سلبيات مثل هذا الانتشار، باعتباره يهدد استقرار النظام العالمي، فإذا كان النظام ثنائي القطبية، وفقاً للبعض، يتسم بدرجة أعلى من اليقين التي تقلل

1-warren Jsamuels, **The Political –Economic logic of world governance**, (Review of social economy, Vol.59, No3, 2001), pp 273-374.

2-Martha Finnemore,"Legitimacy, hypocrisy, and the social structure of unipolarity: why being a unipole isn't all it's cracked up to be", **World politics: Quarterly Journal of International Relations**, Vol16.,No1.,Jan2009, pp. 36 - 64.

3- علي جلال معوض، "إعادة الانتشار: تحليل أولي لأبعاد وآثار انتشار القوة داخل وبين الدول"، **مجلة السياسة الدولية، ملحق اتجاهات نظرية**، عدد رقم (188)، (مركز الأهرام للدراسات السياسية والاستراتيجية، أبريل 2012)، ص ص 18 - 19.

احتمالات الصراع والحروب، مقارنة بالنظام متعدد الأقطاب، فإن النظام القائم على انتشار القوة يحمل احتمالات أكبر لعدم الاستقرار والصراع بأشكال مختلفة[1].

وفي المقابل يوجد اتجاه يرى أن انتشار القوة – مثله في ذلك مثل توازن القوى – لا يقوم بالضرورة على التضاد والصراع، بل قد يكون توافقياً تعاونياً، أو قائماً على التكامل. فانتشار القوة أفقياً ورأسياً يبني الهياكل الهيراركية القائمة على هيمنة الدول القومية، ويخلق تنظيمات شبكية يستمر في إطارها الدور الأساسي للحكومات والدول، ويتزامن ذلك مع زيادة مكانة الفاعلين الآخرين غير الرسميين الذين يقوم بعضهم بجانب من أدوار ووظائف الحكومات. ويسهم ذلك في تطوير معايير جديدة للحكم الرشيد، وتقليل سيطرة الحكومات على حياة الأفراد، لا سيما مع زيادة مصادر قوة قطاعات كبيرة من المواطنين، بفعل تمتعهم بالقوة المعلوماتية المرتبطة بتدفق المعلومات وتداولها.

وفي هذا الإطار يمكن القول إن الفضاء الإلكتروني يتميز بأن له عدة خصائص ساعدت في انتشاره والاعتماد المتزايد عليه منها انخفاض التكلفة الاقتصادية، والسرعة في تبادل المعلومات، وسهولة استخدامه، فضلاً عن إمكانية تخفي الفاعلين الذين يستخدمونه وعدم الكشف عن هويتهم الحقيقية، وهو ما جعل الفضاء الإلكتروني بيئة جاذبة لمستخدميها سواء كانوا أفراداً أو جماعات، مؤسسات رسمية أو غير رسمية، دولاً أو فاعلين من غير الدول، ودفعتهم إلى توظيفه في مختلف المجالات السياسية والاقتصادية والاجتماعية والعسكرية.

وكان نتيجة لذلك تنوع وزيادة عدد الفاعلين المستخدمين للفضاء الإلكتروني، وتعدد مجالات استخدامه ووظائفه، فلم يعد يقتصر على تبادل المعلومات، حيث يستطيع أحد مستخدمي الفضاء الإلكتروني أن يوقع خسائر فادحة بالطرف الآخر، وأن يتسبب في شل البينة المعلوماتية والاتصالاتية الخاصة به، وهو ما يسبب خسائر عسكرية واقتصادية، من خلال قطع أنظمة الاتصال بين الوحدات العسكرية وبعضها البعض أو تضليل معلوماتها أو سرقة معلومات سرية عنها، أو من خلال

1- المرجع السابق، ص 22.

التلاعب بالبيانات الاقتصادية والمالية وتزييفها أو مسحها من أجهزة الحواسيب، وعلى الرغم من فداحة الخسائر فإن الأسلحة بسيطة لا تتعدى الكيلو بايتس، تتمثل في فيروسات إلكترونية تخترق شبكة الحاسب الآلي وتنتشر بسرعة بين الأجهزة، وتبدأ عملها في سرية تامة وبكفاءة عالية، وهي في ذلك لا تفرق بين المقاتل والمدني وبين العام والخاص وبين السري والمعلوم[1].

1- إيهاب عبد الحميد خليفة، **الفضاء الإلكتروني وتهديدات الأمن القومي المصر**، (مقال منشور بالمركز العربي لأبحاث الفضاء الإلكتروني)، 22 أغسطس 2013، بتاريخ مطالعة 30 أغسطس 2013، يمكن المطالعة على:
http://www.accronline.com/print_article.aspx?id=15383

ثالثاً: الفواعل الدولية وتوظيف القوة الإلكترونية:

بداية، تجدر الإشارة إلى أن الأفعال وردود الأفعال الدولية والمتمثلة في السياسات والمواقف والاستراتيجيات الخارجية وما يرتبط بها من قرارات وآليات تنفيذية إنما يقوم بها ويتحمل المسؤولية الكاملة عنها من يمكن أن نسميهم بالفاعلين الدوليين، وتشكل سلوكيات هؤلاء الفاعلين على اختلاف دوافعهم وتوجهاتهم العصب المركزي للنظام السياسي الدولي، كما تؤثر بحسم في مجريات العلاقات السياسية الدولية برمتها.

ماذا يقصد بالفاعل الدولي:

وإذا كان الأمر صحيحاً ولا يثور خلاف حوله، فإن من ينطبق عليه وصف الفاعل الدولي ضمن الإطار الذي سبقت الإشارة إليه، يجب أن يكون محققاً لجملة من المعايير الأساسية التالية[1]:

أ- أن يكون لهذا الفاعل الدولي كياناً قابلاً للتحديد، ويقصد بذلك ألا يكون هذا الكيان هلامياً أو هشاً إلى الحد الذي يصعب معه تحديد ملامحه أو التعرف على خصائصه المميزة والتي تؤثر بدرجة أو بأخرى في أدائه على المسرح السياسي الدولي.

ب- وأن يكون حائزاً لذلك القدر من الموارد والإمكانيات الذي يؤهله لاتخاذ القرارات التي يمكن بها أن يدافع عن مصالحه الأساسية في مواجهة الآخرين، ولا يهم هنا أن تكون الوسيلة إلى ذلك هي التعاون أو التنافس أو الصراع أو الحرب أو غيرها.

ج- أن تتوافر لديه القدرة على التفاعل مع غيره من الفاعلين الذي يتشاركون معه الأدوار على المسرح الدولي، وبالصورة التي تجعل لهذا التفاعل موقعاً في حساباتهم وتأثيراً على ما يقيمونه لأنفسهم من توقعات.

د- ويتمتع بالقدرة على الاستمرار على المسرح الدولي لفترة معقولة من الوقت.

1- د. إسماعيل صبري مقلد، **العلاقات السياسية الدولية: النظرية والواقع**، (كلية التجارة، جامعة أسيوط، الطبعة الرابعة، 2004)، ص ص 73 -75.

وبصورة عامة تتسع قائمة الفاعلين الدوليين والمؤثرين على الساحة الدولية لتشمل[1]:

1- الدول القومية

2- المنظمات الحكومية سواء العالمية أو الإقليمية.

3- الفاعلون فوق القوميين مثل الاتحاد الأوروبي.

4- التحالفات الدولية International Alliances سواء اتخذت طابعاً سياسياً أو عسكرياً أو كليهما.

5- المنظمات الدولية غير الحكومية أو العابرة للقوميات كمنظمة الصليب الأحمر الدولية.

6- الجماعات والمنظمات دون مستوى الدول، مثل جماعات المتمردين على حكوماتهم وحركات التحرر الوطني والمنظمات الإرهابية.

7- الشركات الدولية متعددة الجنسية والتي أصبحت تمتلك من الموارد والقدرات ما يفوق إمكانيات بعض الدول.

8- بعض الأفراد ممن تهيأت لهم دون غيرهم إمكانية التحرك على قاعدة واسعة نسبياً من الاتصالات الدولية.

1- المرجع السابق، ص 75.

وعلى الرغم من تعدد استخدامات الفضاء الإلكتروني من الفاعلين الدوليين من الدول وغيرها، فإنه سيتم التركيز على الفواعل من غير الدول كنموذج لانتشار القوة وتراجع سيطرة الدولة على موارد القوة، على النحو التالي:

الشركات متعددة الجنسية:

أصبحت بعض الشركات متعددة الجنسية تمتلك مصادر للقوة تفوق قدرة بعض الدول، ولم يعد ينقصهذة الشركات سوى شرعية ممارسة القوة التي مازالت حكراً على الدول، فمثلاً خوادم شركات جوجل Google... وميكروسوفت Microsoft وآبل Apple المنتشرة في مختلف دول العالم تسمح لها بامتلاك قواعد من البيانات العملاقة، وتستطيع من خلالها استكشاف واستغلال الأسواق والأفراد، بل وكذلكالتأثير في اقتصادات كثير من الدول، وإن أرادت فيمكنها التأثير على قوة الدولة الاقتصادية، حيث تتوجه معظم الدول إلى جذب مثل هذه الشركات الدولية لخلق استثمارات جديدة بها، لأن العائد الاقتصادي من تصدير التكنولوجيا مرتفع جداً[1].

ومن أبرز الأمثلة على قيام الشركات العاملة في مجال الفضاء الإلكتروني بالتأثير على العلاقات الدولية ... الصراع بين شركة جوجل والحكومة الصينية، حيث قامت الأخيرة باختراق حسابات البريد الإلكتروني Gmail الخاصة بالناشطين السياسيين في الصين، وطالبت شركة جوجل بحجب نتائج البحث حول الموضوعات التي تعتبرها الحكومة الصينية حرجة بالنسبة لها، بما يهدد سمعة جوجل العالمية، خاصة في ظل وجود منافسين أقوياء مثل ميكروسوفت، فضلاً عن سعي الحكومة لسرقة بعض حقوق الملكية الفكرية الخاصة بشركة جوجل ... وهو ما دفع الشركة إلى التهديد بالخروج من

1-Steve Lohr, "Global Strategy Stabilized IBM During Downturn,"**New York Times**, April 20, 2010, Accessed on April 20, 2010.

السوق الصينية إن لم تتوقف الحكومة الصينية عن أفعالها[1] ... وقد قامت بتطوير محرك بحث Baidu الصيني حتى تستطيع الصين الاستغناء عن "جوجل".

أما رد الفعل الأمريكي فقد جاء أكثر حسماً ووضوحاً مما جعل بعض الخبراء يصفون الأزمة بين جوجل والصين بأنها الحلقة الجديدة في مسلسل التوتر بين واشنطن والصين، والذي يضم خلافات حول الميزان التجاري والمناخ ومبيعات الأسلحة لتايوان وملف حقوق الإنسان، وقد سارعت إدارة الرئيس الأمريكي باراك أوباما للدفاع عن شركة جوجل، حيث أكد المتحدث باسم الرئاسة دعم أوباما الكامل لحرية الإنترنت، كما طالبت هيلاري كلينتون وزيرة الخارجية الأمريكية آنذاك الصين بتقديم تفسير فيما يتعلق بالاختراقات المذكورة، مؤكدة أن القدرة على العمل بثقة في مجال الإنترنت تعد من الأمور بالغة الأهمية في العصر الحديث[2]، وهو ما دفع الكاتب إلى التساؤل عما إذا كان هذا الخلاف جزءاً من الخلاف الأمريكي الصيني، أم أنه خلاف تجاري بين الحكومة الصينية والشركة الأمريكية؟

وأعلنت شركة جوجل أنه قد تم حجب جميع خدماتها في الصين بما فيها محرك البحث وبريد Gmail وخرائط جوجل، وذلك في الفترة الواقعة بين مساء يوم الجمعة 9 نوفمبر وحتى يوم الأحد 11 نوفمبر، تزامناً مع المؤتمر الثامن عشر للحزب الشيوعي، الذي يعقد مرة واحدة كل عشر سنوات من أجل تعيين قيادة للحكومة الجديدة[3].

1- Joseph S.Nye, Cyber Power. **Op. Cit**, pp 13-15.

2- جريدة الأهرام، 28 يناير 2010.

3- الصين تحجب خدمات «جوجل» عن مواطنيها، **صحيفة الاقتصادية**، بتاريخ 11 نوفمبر، 2012، تم الاطلاع عليه بتاريخ 21 أغسطس، يمكن المطالعة على:

http://www.aleqt.com/2012/11/11/article_708496.html

المنظمات الإجرامية والجريمة الإلكترونية Cyber Crime:

تعتبر المنظمات الإجرامية المتعددة الجنسية، من الفواعل الدولية التي تؤثر في التفاعلات الدولية، والتي غالباً ما تلقى حماية من بعض الحكومات الضعيفة والفاسدة، هذه المنظمات الإجرامية أوجدت لها ساحة على الإنترنت، وأصبحت تقوم بعمليات قرصنة إلكترونية بهدف سرقة المعلومات أو اختراق حسابات بنكية وتحويل الأرصدة منها، أو من خلال وجود سوق سوداء على الإنترنت لبيع معلومات مالية متعلقة بكلمات مرور شخصية وحسابات بنكية وأرقام كروت وبطاقات ائتمان، حيث تكلف الجرائم الإلكترونية الشركات أكثر من ترليون دولار سنوياً[1]، ولما كان من الصعوبة الكشف عن هوية هذه المنظمات لما يتمتع به الفضاء الإلكتروني من قابلية التخفي، فإنه من الصعب مراقبتها أو تتبعها من أجل تقديمها للمحاكمة، وقد قدر التقرير الصادر عن شركة نورتون Norton للأمن الإلكتروني للعام 2011 أن 431 مليون شخص بالغ يتعرضون للجريمة الإلكترونية سنوياً، أي أكثر من مليون شخص يقعون ضحية للجرائم الإلكترونية يومياً، كما يوضح التقرير أن 64% من الأشخاص الذين يقضون ما بين ساعة إلى 24 ساعة في الأسبوع عبر الإنترنت كانوا عرضة للجرائم الإلكترونية[2].

كما أفاد تقدير حكومي رسمي للجرائم الإلكترونية عبر الإنترنت، والذي نشر من قبل جامعة الأمن العام الصينية، أنها كلفت الاقتصاد الصيني أكثر من 46 مليار دولار أمريكي في السنة الماضية وتحديداً من شهر يونيو 2011 إلى شهر يونيو 2012[3].

1- Frederick R. Chang, "**Is Your Computer Secure?**"(Science, Vol 325, July 2009), p550. http://www.sciencemag.org/content/325/5940/550.short

2- **التدرج المروع للجرائم الإلكترونية**، تقرير صادر عن شركة نورتون، بتاريخ دخول20 أغسطس 2013، يمكن المطالعة على:

http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimereport/ar-ae/index.html

3- **جرائم الإنترنت كلفت الصين أكثر من 46 مليار دولار**، (تقرير على موقع المركز العربي لأبحاث الفضاء الإلكتروني)، بتاريخ دخول 20 أغسطس 2013، يمكن المطالعة على:
http://www.accronline.com/article_detail.aspx?id=8296

وهناك أنواع من الجرائم التي يمكن أن تتم بواسطة الفضاء الإلكتروني، وقد يتعرض لها المستخدم، بل قد يكون طرفاً فيها من حيث لا يدري، مثلا[1]:

- انتحال شخصيات وهمية، أو حقيقية، أو انتحال شخصية الموقع.

- الهجوم على مواقع الإنترنت، والتعديل فيها، فقد يدخل أحد المنافسين لموقع شركة منافسة تعرض سلعها، ويتلاعب بالأسعار المعروضة.

- التلاعب في التجارة الإلكترونية، حيث يتم استخدام بطاقات الائتمان استخداماً غير مسموح به، وقد لا يعرف صاحب البطاقة، أن بطاقته أصبحت متداولة بين مجموعة من المجرمين، يستنزفونها من حسابه.

- وهناك الفيروسات التي تعبث بالأنظمة العاملة، وتعطل الأعمال، وتساعد في خلق البلبلة والاضطراب، وعدم الأمان في استخدامات هذه الوسيلة.

- بالإضافة إلى الجرائم الأخلاقية من الجنس والإعلانات عن الرذائل وابتزاز بعض الشخصيات.

1- حسن طاهر داود، **جرائم نظم المعلومات**، (أكاديمية نايف العربية للعلوم الأمنية، الرياض 2000)، ص ص83- 93.

الجماعات الإرهابية:

ومن أبرز الفواعل الدولية التي أصبحت ظاهرة مُلّحة بعد أحداث 11 سبتمبر هي الجماعات الإرهابية، حيث كانت من أبرز الجماعات التي استخدمت الإنترنت في عمليات التجنيد والتعبئة، واستغلت الفضاء الإلكتروني كمنبر لنشر أفكارها وجذب مؤيدين ومتطوعين لها، وأصبح المنصة الإعلامية لنشر بياناتها وتعليماتها لمجنديها، وإن لم يتعد الأمر لدى هذه الجماعات مرحلة الدعاية والتجنيد، فإنه يظل بإمكانها اختراق شبكات الكهرباء والطاقة والمواصلات، بل والمفاعلات النووية والأسلحة الموجهة إلكترونياً أو عبر الأقمار الصناعية والسيطرة عليها أو تدميرها، الأمر الذي قد يسبب كارثة بشرية.

وتعد ممارسة القوة عبر الإنترنت إرهاباً إذا صاحبتها دوافع سياسية، مثل التأثير على القرارات الحكومية أو الرأي العام، ويتم ذلك من خلال ثلاثة أبعاد مهمة، يتمثل **أولها** في توفير المعلومات عن الأهداف المنشودة لتنفيذ عمليات إرهابية تقليدية، فهو مساعد للإرهاب التقليدي، أو كوسيط في عملية التنفيذ، أما **البعد الثاني** فيستخدم فيه الفضاء الإلكتروني للتأثير على المعتقدات مثل التحريض على بث الكراهية الدينية وحرب الأفكار، أما **البعد الثالث** فيتم في صورة رقمية، حيث تقوم الجماعات المتطرفة على اختلاف أشكالها باستغلال مزايا الفضاء الإلكتروني كعنصر حيوي لدعم وتحقيق أهدافها ومنفذ لوجستي داعم وحاضن لنشاطها الإعلامي في مناطق مختلفة من العالم[1].

فبفضل الفضاء الإلكتروني تحولت القاعدة من تنظيم مقيد بإقليم جغرافي وإمكانيات إعلامية محدودة، إلى تنظيم عابر للأقاليم وللحدود ووسائل الإعلام، وقد حصلت القوات الأمريكية على بعض أجهزة الكمبيوتر المحمول الخاصة بأعضاء تنظيم القاعدة في أفغانستان، وقد وجدت عليها نماذج لسدود مائية، ومفاعلات

1- عادل عبدالصادق، **الإرهاب عبر الإنترنت.. تحديات وفرص المواجهة**، (المركز العربي لأبحاث الفضاء الإلكتروني، تاريخ 20 أغسطس 2013)، يمكن المطالعة على الرابط التالي:
http://www.accronline.com/article_detail.aspx?id=2762

نووية وبعض ملاعب الكرة في أوروبا والولايات المتحدة، وعلى الرغم من وجود دليل على سعي القاعدة لتنفيذ هجمات إلكترونية نحو هذه الأهداف، وأن استخدام الإنترنت كان للتواصل لتنفيذ هجمات إلكترونية نحو هذه الأهداف[1]، فإن السؤال يظل مطروحاً: ماذا يحدث إذا استطاعت هذه الجماعات توجيه هجمات إلكترونية نحو هذه الأهداف؟

حركات التحرر الوطني:

من أبرز الأمثلة على الفواعل الدولية من غير الدول حركات التحرر الوطني، وإن كان يشارك هذه الحركات عدد كبير من الأفراد بصفاتهم الشخصية، ويقومون بإرسال هجمات إلكترونية ضد أهداف العدو على الإنترنت، دفاعاً عن قضية، فمثلاً في أبريل 2013 قام مجموعة من الشباب الفلسطيني والعربي والمؤمن بالقضية الفلسطينية في شتى أنحاء العالم بشن حرب إلكترونية على المواقع الإسرائيلية، تمكنوا فيها من الحصول على ملفات سرية من خلال اختراق الشبكات وتلغيمها، والحصول على أسماء أفراد من الجيش الإسرائيلي ووحدات وأرقام سرية لمئات من الإيميلات، وحسابات فيسبوك، وحسابات كثيرة لرجال أعمال إسرائيليين، وأكثر من 500 حساب مصرفي، كما تم تحميل نحو ألف وثيقة سرية خاصة بالسلطات الإسرائيلية[2].

1- Gabriel Weimann, **Cyberterrorism: How Real Is the Threat?,** (United States Institute Of Peace, December 2004), pp 8-9.

2- هاكر جزائري يكشف تفاصيل الحرب الإلكترونية على إسرائيل، **موقع العربية نت**، تاريخ 10 أبريل 2013، بتاريخ 21 أغسطس 2013.

http://www.alarabiya.net/ar/north-africa/algeria/2013/04/10/%D9%87%D8%A7%D9%83%D8%B1-%D8%AC%D8%B2%D8%A7%D8%A6%D8%B1%D9%8A-%D9%8A%D9%83%D8%B4%D9%81-%D8%AA%D9%81%D8%A7%D8%B5%D9%8A%D9%84-%D8%A7%D9%84%D8%AD%D8%B1%D8%A8-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-%D8%B9%D9%84%D9%89-%D8%A5%D8%B3%D8%B1%D8%A7%D8%A6%D9%8A%D9%84.html

الفرد كفاعل دولي:

أصبح الفرد عنصراً فاعلاً في التفاعلات الدولية، وأصبح يمارس من الأنشطة عبر الفضاء الإلكتروني ما يؤثر به في العلاقات الدولية، ومن أبرز النماذج على ذلك ظاهرة الويكيليكس "Wikileaks phenomena"، حيث نجح ويليام أسانج في نشر الملايين من الوثائق الخاصة بوزارة الخارجية الأمريكية، حيثُ تم استغلال شبكة الإنترنت العالمية في تسريب وثائق تحوي معلومات سرية للغاية مُتداولة بين الإدارة الأمريكية وقُنصلياتها الخارجية بدول العالم الأمر الذي جعل علاقة الولايات المتحدة مع بعض الدول عرضة للتأثر والتهديد، وقد حكمت المحكمة العسكرية بالولايات المتحدة الأمريكية على الجندي برادلي مانينج الذي قام بتهريب الوثائق لوليام أسانج، بالسجن لمدة 35 عاماً على خلفية تسريب معلومات لموقع ويكيليكس[1].

نجح الفضاء الإلكتروني في خلق قنوات اتصال بين بعض المنظمات أو الأفراد وشبكة كبيرة من مستخدمي الفضاء الإلكتروني، خاصة من خلال مواقع التواصل الاجتماعي، كان لها دور بارز ومهم في تنظيم العديد من التظاهرات في مختلف دول العالم، وكانت بمنزلة نافذة إعلامية دولية لمختلف الأفراد الذين يواجهون انتهاكات حقوق الإنسان، كما ساعد على قيام بعض الأشخاص بارتكاب أعمال قرصنة أو جرائم إلكترونية وسرقة معلومات وبيانات شخصية والتلاعب فيها أو إساءة استغلالها.

ومن أبرز مجموعات القرصنة على الفضاء الإلكتروني مجموعة "أنونيموس Anonymous" وهي مجموعة غير مركزية من القراصنة المنتشرين في العالم ذات ثقل كبير في ما يسمى بالحرب الإلكترونية، فكانت على سبيل المثال مسؤولة عن تسريب آلاف رسائل البريد الإلكتروني الخاصة بالرئيس السوري بشار الأسد، كما هاجمت مواقع حكومية أميركية وبريطانية وأخرى للناتو قبل أن تعلن مؤخراً مهاجمتها مواقع حكومية إسرائيلية تعاطفاً مع أهالي قطاع غزة الذين يتعرضون لحملة عسكرية جديدة،

1- أمريكا: السجن 35 عاماً لمسرب "ويكيليكس"، **موقع CNN**، بتاريخ 21 أغسطس 2013، يمكن المطالعة على:
http://arabic.cnn.com/2013/world/8/21/nning-Sentencing-Courtroom-URGENT-1/index.html

وقد تأسست المجموعة عام 2003 عبر منتدى "chan4" الذي يعرض الأعضاء فيه مشاركاتهم من دون الإشارة إلى هويتهم ولا يتطلب التسجيل للمشاركة فيه، لتمثل المجموعة حسب تصورها الدماغ الرقمي العالمي الفوضوي لمجتمع مستخدمي الإنترنت الذين يوجدون في وقت واحد ويتبنون مبدأ المعارضة الشديدة للرقابة على الإنترنت[1].

وقد قامت مجموعة أنونيموس باختراق بيانات شخصية بينها أرقام بطاقات ائتمان تخص الآلاف من عملاء شركة تختص بتحليل المخاطر الاقتصادية والسياسية والعسكرية، وقالت المجموعة في بيان لها إنه من بين العملاء الذي اخترقت حساباتهم وزارة الدفاع الأمريكية وأجهزة أمنية رسمية ومتعاملون أمنيون ومنظمات إعلامية[2].

1- أنونيموس .. الفراصنة المجهولون، **موقع الجزيرة**، بتاريخ 5 فبراير 2013، تاريخ دخول 21 أغسطس 2013http://www.aljazeera.net/news/pages/063cb2e9-5134-4509-a278-6eab43f8bd65?GoogleStatID=9

2- قراصنة كمبيوتر يسرقون معلومات شخصية منشركة أمنية أمريكية، **موقع BBC**، بتاريخ 11 ديسمبر 2013، بتاريخ مطالعة 21 أغسطس،

http://www.bbc.co.uk/arabic/scienceandtech/2011/12/111225_hackers_us_security.shtml

الخلاصة:

مما سبق نستنتج أن الفضاء الإلكتروني ساعد على انتشار القوى بين مختلف الفاعلين، وأعطى مساحة متزايدة للفواعل من غير الدول للتأثير في التفاعلات الدولية، وكان نتيجة لهذا الانتشار أن زادت المخاطر والتهديدات التي تواجهها الدول عبر الفضاء الإلكتروني، وأصبح من الضروري امتلاك مصادر التكنولوجيا الحديثة التي تمكن الدول من مواجهة هذه المخاطر، بل وامتلاك الأسلحة الإلكترونية التي يتم استخدامها.

المبحث الثالث

عناصر القوة الإلكترونية وأبعاد استخدامها في التفاعلات الدولية

بدأ التركيز على الفضاء الإلكتروني كتهديد أمني جديد بفعل أحداث دولية كان أبرزها استخدام تنظيم القاعدة له كساحة قتال ضد الولايات المتحدة، وفي عام 2007 برز بوضوح دور الفضاء الإلكتروني كمجال جديد في العمليات العدائية في الصراع بين روسيا وإستونيا وكذلك في عام 2008 في الحرب بين روسيا وجورجيا، وجاء الهجوم بفيروسي "ستاكسنت Stuxnet" عام 2010 و"فليم Flame" عام 2012 على البرنامج النووي الإيراني ليمثل نقطة مهمة في تطور الأسلحة الإلكترونية، وفي هذا الإطار يسعى هذا المبحث إلى معرفة عناصر القوة الإلكترونية وأبعاد استخدامها في إدارة العلاقات الدولية.

أولاً: عناصر القوه الالكترونيه:

> **تتركز عناصر القوة الإلكترونية في 6 عناصر رئيسية، تشمل وجود بنية تحتية تكنولوجية والقدرة على تطوير أسلحة إلكترونية وإدارة عمليات عبر الفضاء الإلكتروني تشمل مهاجمة شبكات الخصم والدفاع عن الشبكات الوطنية واستطلاع الشبكتين، بالإضافة إلى وضع خطة استراتيجية تحدد الأهداف والآليات والمؤسسات المنوط بها توظيف القوة الإلكترونية، مع وجود عنصر بشري مدرب وقادر على استخدامها.**

كان نتيجة لاتجاه الصراع الدولي حول الموارد والمصالح والقيم، نحو الاعتماد المتزايد على تكنولوجيا الاتصال والمعلومات، أن أصبح الفضاء الإلكتروني ساحة جديدة للصراع بشكله التقليدي ولكنه ذو طابع إلكتروني يتجاوز الحدود القومية وسيادة الدول، ويسعى كل طرف من طرفي الصراع إلى تحقيق أكبر مكاسب وإلحاق أكبر قدر من الخسائر بالطرف الآخر، ويتميز الصراع الإلكتروني بأن به تدميراً لا تصاحبه دماء أو أشلاء، ويتضمن التجسس والتسلل ثم النسف لكن لا دخان ولا أنقاض ولا غبار، وتتميز أطرافه بعدم الوضوح وتكون تداعياته خطيرة سواء عن طريق تدمير قواعد البيانات الموجودة على الإنترنت ونسفها أو قصفها بوابل من الفيروسات أو العمل على استخدام أسلحة الفضاء الإلكتروني المتعددة للنيل من سلامة المواقع الإلكترونية وقواعد البيانات، وهي أسلحة يسهل الحصول عليها من خلال مواقع الإنترنت وتعلم كيفية استخدامها[1]، ونتج عن ذلك ظهور شكل جديد من الحروب، يكون في وسط الشعوب، بعيداً عن الساحات التقليدية للصراع الدولي، هذا الشكل هو "الحرب الإلكترونية".

1- عادل عبد الصادق، **الإرهاب الإلكتروني، القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة**، المرجع السابق، ص ص 2-4.

ويُنظر إلى الحرب الإلكترونية باعتبارها "القدرة على الدفاع عن والهجوم على المعلومات، من خلال شبكات الحاسب الآلي عبر الفضاء الإلكتروني، بالإضافة إلى شل قدرة الخصم على القيام بهذه الهجمات نفسها"، حيث يرى كينث جريس أن الحرب الإلكترونية تشمل خمسة عناصر رئيسية هي التجسس، الدعاية، الحرمان من خدمة الإنترنت، تعديل البيانات والتلاعب بها، والتلاعب أيضاً بالبنية التحتية[1].

وتتركز عناصر القوة الإلكترونية لدولة ما في ستة محاور رئيسية هي:

1- بنية تكنولوجية Cyber Infrastructure

2- الأسلحة الإلكترونيةCyberWeapons

3- إدارة العمليات الإلكترونية Computer Network Operations(CNO) **والتي تشمل:**

- مهاجمة شبكات الحاسب الآلي Computer Network Attack (CNA)
- الدفاع عن شبكات الحاسب الآلي Computer Network Defense (CND)
- استطلاع شبكات الحاسب الآلي Computer Network Exploitation (CNE)

4- بنية مؤسسية وتشريعية Institutional And Legal Framework

5- خطة استراتيجية لتوظيف القوة الإلكترونية

6- العنصر البشري Human Resources

1 - Kenneth Geers, **Cyber Space and the changing nature of warfare**,(U.S. Representative Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia). On http://www.carlisle.army.mil/DIME/CyberSpace.cfm On August 15, 2013.

1- بنية تحتية تكنولوجية:

وهي بمنزلة البنية التحتية اللازمة للقوة الإلكترونية، فبدلاً من الدبابات والطائرات والغواصات، تحتاج الدولة في هذا النوع إلى أجهزة كمبيوتر، وشبكات اتصالات مرتبطة بأجهزة الكمبيوتر وببعضها البعض، وبرمجيات، بالإضافة إلى العنصر البشري المدرب على استخدام هذه الأجهزة والشبكات.

وإذا كانت الدولة تمارس نوعاً من التأثير في الإقليم البري والجوي والبحري من خلال قوتها العسكرية المادية، فإنها تستطيع أن تمارس نوعاً من التأثير أيضاً من خلال بنيتها المعلوماتية والتكنولوجية في الفضاء الإلكتروني[1].

وتتضح معالم هذه البنية التكنولوجية في جميع مؤسسات وخدمات الدولة والتي تشمل:

أ- الأنظمة المالية والمصرفية:

بما يوفره الفضاء الإلكتروني والشبكات الإلكترونية من سرعة ودقة في تنفيذ العمليات المالية والمصرفية، وتيسير سبل الدفع عبر المنصات الإلكترونية من دون الحاجة إلى التوجه إلى المؤسسات والشركات، ومن دون الاعتراف بحدود جغرافية، وهو ما يدعم بصورة مباشرة قطاع الاستثمارات والسياحة.

1- Miller and Kuehl, "Cyberspace and the 'First Battle' in 21st-century War," Eugene Habiger, **Cyberwarfare and Cyberterrorism: The Need for a New U.S. Strategic Approach**, (Washington DC: Cyber Secure Institute, February 1, 2010), p 2.

ب- شبكات الكهرباء والطاقة:

حيث تعتمد هذه الشبكات على نظم إدارة إلكترونية عملاقة مثل نظام SCADS الذي يستخدم في إدارة السدود المائية العملاقة ومحطات الكهرباء والطاقة النووية، وغيره من النظم الإلكترونية التي تضمن تحقيق سبل السلامة في إدارة هذه المنشآت الحيوية.

ج- نظم إدارة الخدمات العامة:

والتي تشمل المستشفيات والمدراس والمواصلات والاتصالات وغيرها من الخدمات العامة التي يمكن ربطها إلكترونياً بحيث توفر الجهد وتحقق الكفاءة في الإدارة.

2- أسلحة الإلكترونية:

وهي برامج تم تصميمها للقيام بوظائف مختلفة وتشمل:

أ- فيروسات الحاسوب Viruses:

وهي برامج خارجية صُنعت عمداً بغرض تغيير خصائص الملفات التي يصيبها لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب وما شابهها من عمليات، أي أن الغرض منها هو إلحاق الضرر بحاسوب آخر أو السيطرة عليه، وتتم كتابتها بطريقة معينة، وقد تستخدم الفيروسات لتعطيل شبكات الخدمات والبنية التحتية لطرف المستهدف كأن يتم عن طريقها إحداث فشل في شبكة الاتصالات لدولة ما[1].

1-**What is a computer virus?**, http://www.microsoft.com/security/pc-security/virus-whatis.aspx On august 10, 2013.

ب- الديدان Worms:

هي برامج صغيرة لا تعتمد على غيرها وتتكاثر بنسخ نفسها عن طريق الشبكات، صنعت للقيام بأعمال تخريبية كأن تعمل على قطع الاتصال بالشبكة أو سرقة بعض البيانات الخاصة بالمستخدمين أثناء تصفحهم الإنترنت، وتمتاز بسرعة الانتشار ويصعب التخلص منها نظراً لقدرتها الفائقة على التلون والتناسخ والمراوغة. وغالباً عندما تستخدم في حروب المعلومات تستهدف الشبكات المالية التي تعتمد على الحاسوب، مثل شبكات البنوك[1].

ج- أحصنة طروادة Trojan Horses:

هي شيفرة أو برنامج صغير مختبئ في برنامج كبير من البرامج ذات الشعبية العالية، ويقوم ببعض المهام الخفية كأن يعمل على نشر دودة أو فيروس، وهو مبرمج بمهارة عالية إذ لا يمكن اكتشاف وجوده، حيث يعمل دائماً على مسح آثاره التي لا تحمل صفة تخريبية، وغالباً ما يعمل على إضعاف قوى الدفاع لدى الضحية ليسهل اختراق جهازه وسرقة بياناته كأن يقوم مثلاً بإرسال بيانات عن الثغرات الموجودة في نظام ما، وكذلك إرسال كلمات المرور السرية الخاصة بكل ما هو حساس من مخزون معلومات الطرف المستهدف[2].

1- **Computer worms,**http://virusall.com/computer%20worms/worms.php On august 10, 2013.
2-**Trojan horse**,http://searchsecurity.techtarget.com/definition/ On 10 August.

د- القنابل المنطقية Logic bombs:

تعد نوعاً من أنواع أحصنة طروادة، حيث يزرعها المبرمج داخل النظام الذي يطوره، وقد تكون برنامجاً مستقلاً، وتُصمم بحيث تعمل عند حدوث أحداث معينة أو تحت ظروف معينة أو لدى تنفيذ أمر معين، وتؤدي إلى تخريب أو مسح بيانات أو تعطيل النظام لطرف المستهدف[1].

هـ- الأبواب الخلفية Backdoors:

هي ثغرة تُترك عن عمد من قبل مصمم النظام؛ لكي يستطيع الدخول إلى النظام عند حاجته لذلك، حيث تقوم كبريات الدول المصدرة للبرمجيات بترك أبواب خلفية تستخدمها عند الحاجة، وهو ما يمكن هيئات وأركان حرب المعلومات من التجوال الحر داخل أي نظام لأي دولة أجنبية[2].

و- الرقائق Chipping:

ممن الممكن أن تحتوي بعض الرقائق الإلكترونية على وظائف غير متوقعة أو معروفة كما في البرامج والنظم، حيث يمكن للدوائر المجمعة التي تشكل هذه الرقائق أن تحتوي على وظائف إضافية أثناء تصنيعها، لا تعمل في الظروف العادية، إلا أنها قد تعلن العصيان في توقيت معين، أو بالاتصال بها عن بعد، حيث يمكن أن تستجيب لتردد معين لبعض موجات الراديو، فتشل الحياة في مجتمع أو دولة ما[3].

1-Ibid.
2-Ibid.
3- Ibid.

ز- الماكينات والميكروبات فائقة الصغر:

ويطلق عليها (Nano Machines And Microbes)، وهي عكس الفيروسات، حيث إنها تصيب عتاد النظام (Hardware) فالـ(Nano Machines)عبارة عن (Robots) فائقة الصغر قد تنتشر في مبنى نظام معلوماتي في دولة معادية أو منافسة؛ حيث تتفشى في الطرقات والمكاتب حتى تجد حاسباً آلياً، وتدخل إليه من خلال الفتحات الموجودة به، لتبدأ عملها بإتلاف الدوائر الإلكترونية.

أما الميكروبات (Microbes) فمن المعروف أن بعضاً منها يتغذى على الزيت، فماذا إذ تم تحويرها جينيًّا لتتغذى على عنصر الـــ(Silizium) المكون المهم في الدوائر الإلكترونية فإن هذا يعني تدمير وإتلاف الدوائر الإلكترونية في أي معمل توجد فيه حاسبات آلية أو حاسب خادم (Server) لموقع على الإنترنت، أو مبنى مهم أو حساس يدار بالكمبيوتر، أو حتى مدينة بأسرها عن طريق إتلاف دوائر التحكم الإلكترونية فيها.

ح- مدافع HERF :

عبارة عن مدافع تطلق موجات راديو مركزة وعالية الطاقة والتردد (High Energy Radio Frequency) والتي يمكنها تعطيل وإتلاف أي هدف إلكتروني، أما مستويات الضرر التي قد تحدثها فهي تختلف من ضرر متوسط كغلق شبكة حاسب مثلاً أو إعادة تشغيله بشكل دوري فلا يمكن استغلاله، إلى ضرر بالغ كإعطاب العتاد الخاص بالحاسب أو الشبكة بشكل لا يمكن بعده إصلاح الحاسب أو الشبكة[1].

1-**HERF gun zaps more than your dinner**, On July 20, 2013http://hackaday.com/2011/03/21/herf-gun-zaps-more-than-your-dinner/

ط- قنابل EMP:

هي تشبه المدافع غير أنها تستخدم نبضات إلكترومغناطيسية Electromagnetic Pulse)، حيث يمكن التسلل إلى مواقع العدو الإلكترونية الحساسة والمهمة وإلقاء هذه القنابل التي سوف تتلف كل الحواسب والشبكات في دائرة انفجارها غير المدوي أو المشتعل، وهي وإن كانت أصغر حجماً من مدافع HERF إلا أنها أوسع وأبعد أثراً؛ حيث إنها لا تنتقي هدفاً معيناً، بينما قذيفة مدفع HERF تنتقي هدفها[1].

3- العمليات الإلكترونية:

وتنقسم إلى ثلاثة أنواع رئيسية هي:

أ- مهاجمة شبكات الحاسب الآلي (Computer Network Attack, CNA):

وتشمل اختراق الشبكات لحقن الحاسبات بكمٍ هائل من البيانات لتعطيلها أو وضع بيانات ومعلومات محرفة لإرباك مستخدمي الحاسبات، ونشر الفيروسات (Viruses) وما شابهها من البرامج الصغيرة المؤذية مثل الديدان (Worms)، وتلغيمها بالقنابل المنطقية (Logic Bombs) التي يتم تنشيطها في الوقت المناسب للمهاجم لكي تتلف ما تحتويه الحاسبات من بيانات وبرمجيات، أو القيام بهجمات إلكترونية أو مادية لقطع لخدمات الإنترنت Denial Of Service Attacks عن الخصم ومن ثم القدرة على تدمير قواعد البيانات الإلكترونية التي يمتلكها، وتعطيل قدرته على النشر السريع لقدراته وإمكانياته وقواته، أو قطع أنظمة الاتصال بين الوحدات العسكرية وبعضها وتعطيل شبكات الكمبيوتر، أو شل أنظمة الدفاع

1-**"Emp 101"A Basic Primer & Suggestions For Preparedness**http://www.onesecondafter.com/pb/wp_d10e87d9/wp_d10e87d9.htmlOn 20 July 2013.

الجوي أو التوجيه الإلكتروني للخصم، أو السيطرة على وحدات القيادة والتوجيه، أو فقدان العدو قدرته على التحكم أو الاتصال بالأقمار الصناعية[1]، وقد يصل الأمر إلىالتدمير الفعل (Physical Destruction) من خلال تدمير الجانب المادي مثل الخادمات والأسلاك والكابلات والأجهزة التي تحتوي على معلومات يصعب التأثير عليها من بعد، وتتم عملية التدمير بالأسلحة التقليدية كالجوية والبحرية والبرية أو بعمليات القوات الخاصة.

ب- الدفاع عن شبكات الحاسب الآلي Computer Network Defense (CND):

وتشمل هذه العملية حماية الشبكات وأجهزة الكمبيوتر من أي عملية اختراق خارجي، ويجب أن يكون التأمين على مستوى البرمجيات Software والمكون المادي للشبكات Hardware، بحيث يتم تأمين الشبكة من أي اختراق خارجي بأي من الأسلحة الإلكترونية السابق ذكرها، وكذلك تأمين المكون المادي للشبكات، مثل الخوادم أو الشرائح الإلكترونية، والتي قد تكون مبرمجة من قبل المصمم لكي تعمل في ظروف غير عادية لصالحه[2].

ج- استطلاع شبكات الحاسب الآلي Computer Network Exploitation (CNE):

وتعني القدرة على الدخول غير المشروع والتجسس على شبكات الخصم، دون أن يصاحب ذلك تدمير أو تخريب للبيانات والمعلومات، بهدف الحصول على هذه المعلومات والتي قد تشمل خطط دفاع وهجوم عسكري، أو أسرار عسكرية وحربية،

1- Colonel Jayson M. Spade, **China's Cyber Power And America's National Security**, Jeffrey L. Caton Editor, (U.S. Army War College, May2012) p 7.
2-Ibid, 9.

أو معلومات سياسية واستخباراتية، ولا تتوقف وظيفتها على ذلك فحسب، بل يمكن من خلالها عمل خرائط لشبكات الحاسب الآلي واستخدامها مستقبلاً في عمليات الهجوم الإلكتروني، كما يمكن ترك بعض الثغرات من خلال الأبواب الخلفية Backdoors لحقن الشبكة بفيروسات للقيام بمهام معينة، مثل نقل البيانات إلى أجهزة المتجسس[1]، كما يمكن أيضاً استخدامها في التأثير على أفكار وسلوكيات الخصم من قبيل الحرب النفسية، وذلك بنشر مثل هذه الخطط العسكرية والبيانات أو إرسالها إليه مرة أخرى لكي يدرك إلى أي مدى هو مُخترق ولن يستطيع المواجهة، مما يدفعه إلى الاستسلام أو التفاوض.

4- بنية مؤسسية وتشريعية Institutional And Legal Framework

ويقصد بها وجود جهة مؤسسية تعمل على تحقيق استخدام القوة الإلكترونية لتحقيق أهداف الدولة الاستراتيجية، كوكالة الأمن القومي الأمريكي ووحدة عمليات الفضاء الإلكتروني الأمريكية، أو تدريب جيش من القراصنة المحترفين للمساهمة في تحقيق أهداف الدولة، أو إنشاء الكتائب الإلكترونية مهمتها الدفاع عن مصالح الدولة، بالإضافة إلى ذلك وجود هيكل تشريعي يحدد الجرائم الإلكترونية ويُعرفها ويضع العقوبات اللازمة على مرتكبيها، بهدف الحفاظ على النظم الإلكترونية الموجودة بالدولة، وتحقيق الأمن الإلكتروني للأفراد، منعاً لوقوعهم ضحايا لعمليات نصب إلكتروني[2].

1- Dennis M. Murphy, ed., **Information Operations Primer,** (Carlisle, Pennsylvania: U.S. Army War College, 2010), p 169.

2- القاضي أحمد حاتم محمد سعيد أحمد جعفر، **الأطر التشريعية والقانونية لأمن وسلامة الفضاء السيبراني في مصر**، (بيروت : المركز العربي للبحوث القانونية والقضائية)، ص ص 3 – 5.

5- وجود خطة استراتيجية تدعم رؤية الدولة لتعظيم قوتها الإلكترونية:

إن امتلاك الدولة قدرات إلكترونية وعنصراً بشرياً مدرباً ومؤسسات مسؤولة عن توظيف القوة الإلكترونية، من دون جود خطة استراتيجية للدولة تضع الأهداف وآليات التنفيذ، وتحدد الوظائف الرئيسية لكل جهة، يؤدي إلى إهدار الموارد، وتضارب الاختصاصات، وعدم تحقيق الهدف الرئيسي للدولة سواء بحماية أمنها الإلكتروني أو شن هجمات إلكترونية على أهداف عدائية، فكان من الضروري لأي دولة تسعى لامتلاك قوة إلكترونية أن تضع خطة استراتيجية خاصة برؤيتها لمصالحها وأهدافها التي تسعى لتحقيقها، ودور المؤسسات المنوط بها استخدام القوة الإلكترونية لتحقيق هذه الأهداف، سواء كانت أهدافاً هجومية أو دفاعية.

6- العنصر البشري Human Being

لكي تستطيع دولة ما أن تمتلك قوة إلكترونية مؤثرة، وتستطيع أن توظفها في تحقيق أهدافها، لابد من توافر عنصر بشري مدرب ومتعلم وقادر، ليس فقط على استخدام تكنولوجيا الاتصال وحسب، بل أيضاً اختراعها وتطويرها، وتوفير هذا العنصر مرتبط بصورة أساسية بجودة التعليم من ناحية، ودرجة الإقبال على المواد الرياضية والهندسية من ناحية أخرى، يُضاف إلى ذلك ولاء العنصر البشري الذي يتعامل مع النظم الإلكترونية، حتى لا يقوم بعمل ثغرات في النظم الإلكترونية يستفيد منها خصوم الدولة أو الشركة أو المؤسسة التي يعمل لديها، أو أن يقوم بتسريب ملفات غاية في السرية قد تتسبب في وقوع أضرار مالية أو مادية[1].

وغالباً ما يطلق على المبرمج القادر على اختراق النظم الأمنية في الفضاء الإلكتروني أو اكتشاف الثغرات ومعالجتهم اسم قرصان أو هكر Hacker ويشير المصطلح إلى الشخص الذي يسعى إلى معرفة كل شيء عن أنظمة الكمبيوتر، ويحاول أن يجد حلولاً ليجعلها تعمل بكفاءة أعلى أو أن تقوم بمهام ليس من المفترض أن تقوم بها، عكس الأفراد التقليديين الذي يسعون إلى معرفة الضروريات فقط التي يحتاجون إليها.

1- Franklin D. Kramer, Cyber Power And National Security, **Op .Cit**, p8.

والهاكرز بصفة عامة ثلاثة أنوع يمكن تقسيمهم كالتالي:

أ- الهاكر ذو القبعة البيضاء (White Hat Hacker):

ويطلق على الهاكر الصالح، وهو ذلك الشخص الذي يستخدم قدراته في مجال الكمبيوتر بصورة شرعية، لا يترتب عليها الإضرار بمصالح الغير، ويحاول أن يجد الثغرات في أنظمة الكمبيوتر بهدف تأمينها من محاولات الاختراق الخارجية.

ب- الهاكر ذو القبعة السوداء (Black Hat Hacker):

ويطلق على الهاكر المفسد، وهو يسمى بالإنجليزيةCracker، للتمييز بينه وبين الهاكر الصالح، وهو الشخص الذي يستغل قدراته للإضرار بمصالح الآخرين، أو لتحقيق أهداف غير شرعية، كسرقة البنوك والبطاقات الائتمانية واختراق مواقع الإنترنت لكسب المال.

ج- الهاكر ذو القبعة الرمادية (Grey Hat Hacker):

وهو ذلك الشخص المترنح بين الإصلاح والعبث، فهو تارة يقوم بتأمين وحماية أنظمة الكمبيوتر، وتارة أخرى يقوم باختراقها لتحقيق أهداف شخصية.

ولعل تلك التسميات جاءت من الأفلام الغربية القديمة، التي كان يرتدي فيها الأفراد الصالحون القبعات البيضاء، والمفسدون القبعات السوداء.

مستويات الهاكر :

أ- مبتدئ: Script kiddies

ويمكن أن يُطلق عليه "مشروع هاكر"، فهو الشخص الذي يستخدم الأدوات المطورة بواسطة الهاكر من أجل القيام بعملية قرصنة محدودة على أنظمة كمبيوتر، وغالباً ما تكون مهاراته ضعيفة، ويمكن مواجهة محاولات اختراقه في بدايتها.

ب- متمرن: Intermediate Hackers

وهم الأشخاص الذين لديهم مهارات برمجية كافية في أنظمة الكمبيوتر والشبكات، ويعلمون ما يمكن أن يقوم به كود معين لتحقيق وظيفة معينة، ولكن مثل الفئة السابقة، عادة ما يستخدمون برامج وأكواد معروفة نسبياً، ويعتمدون على الثغرات الموجودة في الأنظمة لمحاولات اختراقها.

ج- محترف: Elite Hackers

وهم الأشخاص المهرة والموهوبون في استخدام الكمبيوتر واستطلاع شبكات الإنترنت، ويقومون بعملية تصميم برامج القرصنة الإلكترونية، ولديهم قدرة على اختراق الأنظمة المؤمنة، ومواجهة محاولات الاختراق الخارجية من قراصنة آخرين، وليس كل القراصنة يمكن أن يصلوا إلى هذا المستوى من الحرفية.

ثانياً: استخدامات القوة الإلكترونية في التفاعلات الدولية:

تصاعد الاهتمام الدولي بالفضاء الإلكتروني، خاصة بعد ما أتاحه من أدوات وآليات جديدة كوسيلة ووسيط لتهديد عمل المرافق الحيوية والبنية التحتية الكونية للمعلومات وعدم توقفها أمام سيادة الدول، بما جعلها بيئة خصبة للاستخدام غير السلمي من جانب كافة الفاعليين على تنوعاتهم المختلفة والذين تراوحوا بين استخدام الدول إلى الفاعليين من غير الدول، وظهر ذلك في استخدم الفضاء الإلكتروني كساحة للحرب الباردة والحرب النفسية وحرب الأفكار أو من خلال استخدامه لشن الحروب والإرهاب بين الدول أو استخدام الأفراد أو الجماعات الإرهابية أو القراصنة أو الجريمة المنظمة وذلك على نحو يؤثر في الطبيعة المدنية أو السلمية للفضاء الإلكتروني.

وقد قامت بعض الدول بإنشاء كتائب أو جيوش من القراصنة الإلكترونيين، حيث وجدت بعض الحكومات، مثل الصينية والروسية والأمريكية، وسيلة للمساهمة في تحقيق أهداف الدولة الاستراتيجية، مثل محاولة اختراق الأنظمة الإلكترونية للدول الأخرى وسرقة البيانات والمعلومات والخطط العسكرية والاستراتيجية، والدفاع عن الشبكات الوطنية للدولة ضد أي محاولة اختراق خارجية.

وهناك اتجاه متزايد للدول لإنشاء وحدات خاصة بالحروب الإلكترونية التي تتم عبر الفضاء الإلكتروني وشبكات الحاسب الآلي، ومن أبرز هذه الوحدات الخاصة بالدول:

الصين: الوحدة 61398:

هي وحدة سرية بجيش التحرير الشعبي الصيني، تقوم بعمليات التجسس الإلكتروني، وسرقة المعلومات الاقتصادية، خاصة من الولايات المتحدة الأمريكية، وتتسم عملياتها بالسرية التامة، ولا يتم الإعلان عنها، وفي تقرير صادر عن شركة "مانديات" الخاصة بالأمن الإلكتروني، أكدت أن الوحدة 61398 بدأت في شن أولى هجماتها منذ عام 2006، وقامت بسرقة مئات من التيرابيتس الخاصة من 141

منظمة تشمل المخططات التكنولوجيا، وعمليات التصنيع والبيانات والوثائق وخطط التسعير والتسويق، ورسائل البريد الإلكتروني وقوائم الاتصال، على الأقل 115 منها في الولايات المتحدة الأمريكية.

وحسب التقرير يُعتقد أن الوحدة 61398 تحت إدارة المكتب الثاني التابع للإدارة الثانية لهيئة أركان جيش التحرير الشعبي، وتقع في منطقة شنغهاي وتقوم شركة الاتصالات الصينية بإمدادها بنوع خاص من الألياف الضوئية لنقل بيانات الإنترنت، ويعتقد التقرير أن الوحدة تضم أو أنها هي نفسها تشكل ما أطلقت عليه مانديت اسم APT1، Advanced Persistent Threat أي التهديد المستمر المتقدم، الذي قام بالهجوم على عدد كبير من المؤسسات الصناعية والحكومية حول العالم منذ عام 2006 على الأقل.

وتعتمد الوحدة 61398 على شبكة من القراصنة الإلكترونيين الصينيين في 13 دولة، يقع معظمها في الولايات المتحدة التي تمتلك أكثر من 100 جهاز كمبيوتر مخصصة لغرض العمليات الإلكترونية، وفي 18 فبراير 2013، أصدرت المخابرات المركزية الأمريكية تقريراً من 60 صفحة يتهم الوحدة 61398 بالوقوف وراء عمليات التجسس والتخريب على الإنترنت، وفي 19 مايو 2014، ولأول مرة في التاريخ وجه المدعي العام الأمريكي إريك هولدر، باسم مكتب التحقيقات الفيدرالي تهماً جنائية بسرقة معلومات تجارية حساسة من خمس شركات أمريكية كبرى (يو إس ستيل، ألكوا، وستنگهاوس، سولار ورلد)، إلى خمسة ضباط في الوحدة 61398 التابعة للجيش الصيني، وطلب من الحكومة الصينية تسليمهم للولايات المتحدة، ودائماً ما تواجه الصين الاتهامات الموجهة إليها من القيام بهجمات إلكترونية أو سرقة معلومات سرية بالنفي، والادعاء بأنها أيضاً ضحية لعمليات قرصنة إلكترونية.

الولايات المتحدة : Cyber CommandUS

استحدث البنتاجون في يونيو 2009 قيادة عسكرية مهمتها الرد على هجمات قراصنة المعلوماتية وتنفيذ عمليات في الفضاء الإلكتروني. وقد تم تعيين أول جنرال عسكري لإدارة حروب الفضاء الإلكتروني هو الجنرال إلكسندر كيث، وتستهدف وزارة الدفاع الأمريكية من تلك القيادة الجديدة أن تشرف على مختلف الجهود المتعلقة بالإنترنت في كل أجهزة القوات المسلحة، سواء من حيث تأمينها أو القيام بعمليات إلكترونية عسكرية ضد أهداف خارجية، وفي كلمه له أكد وزير الدفاع الأمريكي تشاك هيجل أنه من المتوقع أن يصل عدد قوات القيادة العسكرية للفضاء الإلكتروني إلى 6000 مقاتل بحلول عام 2016.

وقبل استحداث هذه القيادة كانت الحكومة الأمريكية تعتمد على وكالة المخابرات المركزية CIA ووكالة الأمن القومي الأمريكي NSA للقيام بعملياتها في الفضاء الإلكتروني، بل إن معظم مشاريع التجسس الإلكتروني الكبرى للولايات المتحدة مثل بريسم PRISM وغيره نفذتها وكالة الأمن القومي.

وتتركز المهمة الرئيسية لهذه القيادة على حماية شبكات وزارة الدفاع وأنظمتها، والاستعداد لخوض الحروب والدفاع عن شبكات الدولة الأمريكية، من خلال إدارة عمليات شبكات المعلومات التابعة لوزارة الدفاع الأمريكي، لتحقيق هدفين رئيسيين هما، حماية حرية عمل الولايات المتحدة وحرية عمل حلفائها في الفضاء الإلكتروني، وحرمان أعداء الولايات المتحدة – عند الطلب- من حرية العمل في الفضاء الإلكتروني.

روسيا: Hacker Network

صرح المتحدث باسم وزارة الدفاع الروسية "ايجور يجوروف" في أكتوبر الماضي أن روسيا تخطط لبناء نظام إلكتروني شامل على مراحل يتم الانتهاء منه عام 2017 لحماية البنية الأساسية للقوات المسلحة من الهجمات الإلكترونية، كما أمر وزير الدفاع

"سيرجي شويجو" الصيف الماضي بإدراج 500 من الطلبة المتميزين في استخدام الحاسب الآلي في "وحدات علمية" خاصة، وسيعتبر عملهم مثل الخدمة العسكرية.

ولكن هذا لا يعني أن روسيا لا تمتلك عناصر بشرية مؤهلة للقيام بالعمليات الإلكترونية، حيث إنها تعتمد على عدد كبير من القراصنة سواء المتطوعون أو الذين يتم توظيفهم لخدمة أغراض روسية عسكرية، حيث قامت روسيا في 2007 بشن حرب إلكترونية شاملة على إستونيا بسبب نقل تمثال يخلد تضحيات جنود روس في الحرب العالمية الثانية، ونتج عنها شل قطاعات البنوك والوزارات وشبكات الاتصالات من خلال هجمات اختراقية سريعة ومدروسة أدت إلى دمار لوجستي كبير، ولم يعد المواطنون قادرين على إجراء معاملاتهم البنكية الإلكترونية التي تتم 97% منها عبر الإنترنت أو التواصل مع بعضهم بالبريد الإلكتروني لأيام عديدة، وتم تعطيل البنية التحتية للاقتصاد الرقمي الإستوني، وكررت ذلك قبل الغزو الروسي لجورجيا عام 2008.

إسرائيل: الوحدة 8200

الوحدة (8200)، وهي أيضاً الوحدة المسؤولة عن قيادة الحرب الإلكترونية في الجيش الإسرائيلي، والتي تم إنشاؤها عام 1952 والتي تشكل تحالفاً مع وكالة الأمن القومي الأمريكي NSA وقيادة الفضاء الإلكتروني US Cyber Command ، وتعتبر أهم وأكبر قاعدة تجسس إلكترونية إسرائيلية بالنقب للتنصت على البث الإذاعي والمكالمات الهاتفية والفاكس والبريد الإلكتروني في قارات آسيا وأفريقيا وأوروبا.

وقد لعبت هذه الوحدة دوراً رئيسياً في ضرب البرنامج النووي الإيراني من خلال تصميم فيروس ستاكسنت Stuxnet الذي أصاب 1000 من أجهزة الطرد المركزي الإيراني وتسبب في تعطيل البرنامج النووي، وقد أكد المعلق العسكري الإسرائيلي عمير رايبوبورت أن الدور الذي تقوم به "وحدة 8200"، التابعة لشعبة الاستخبارات العسكرية الإسرائيلية (أمان)، قد جعل إسرائيل ثاني أكبر دولة في

مجال التنصت في العالم، بعد الولايات المتحدة، وأشار رايبوبورت إلى أن الحواسيب المتطورة التابعة لوحدة 8200 قادرة على رصد الرسائل القيمة الاستخباراتية ذاتها من خلال معالجة ملايين الاتصالات ومليارات الكلمات.

أنماط استخدام القوة الإلكترونية في التفاعلات الدولية:

حدد جوزيف ناي أنماطاً لاستخدام القوة الإلكترونية وميز بين الاستخدام الناعم لها والاستخدام الصلب[1]، وكان نتيجة لاستخدامات القوة الإلكترونية في التفاعلات الدولية أن ظهر بعد جديد لها، وهو الصراع والردع وسباق التسلح على الفضاء الإلكتروني، **ويتضح ذلك في التالي:**

أ- الصراع الدولي على الفضاء الإلكتروني:

فقد تطور الصراع الدولي بشكل هائل نتيجة للتطور الكبير في المعلومات مما جعل هذهِ المعلومات هي الهدف الأساسي الذي تسعى الدول للحصول عليه، فقد مكنت المعلومة الدول من إنتاج السلاح النووي، وظل هذا التطور مستمراً، حيث اعتمدت كل مرحلة من مراحل التطور الإنساني على سلطة أو قوة من طبيعة معينة تتناسب مع متطلبات هذه المرحلة، ولقد أثرت هذه السلطة أو القوة بصورة مباشرة أو غير مباشرة في أدوات الصراع بين المجتمعات وآلياتها، وأفرزت مفردات ومكونات تكاملت معاً لتنتج نظاماً دولياً سيطرت مفاهيمه بعض الوقت أو كل الوقت، وفي هذا الإطار تميز عصرنا الحالي بظاهرة الثورة العلمية والتكنولوجية ولقد أزاحت وحيدت التكنولوجيا الكثير من عناصر القوة عن مواقعها التي تربعت عليها فترة طويلة، مما عرض المفهوم التقليدي للقوة إلى انتقادات، وأفصح عن محتوى جديد للقوة، فلم يعد ما في يد الدولة من قدرات عسكرية أو ما تمتلكه من أموال وثروات، كافياً لبلورة

1- انظر تفاصيل ذلك الجزء في الرسالة، ص ص 23-24.

دورها كقوة مؤثرة وفاعلة، بل إن مسار هذا التغير الذي أحدثته التكنولوجيا في حالة حركة، وهو في طريقه إلى التصاعد وطور التكوين.

ومن غير الممكن فهم العلاقات الدولية وظاهرة الصراع الدولي بمعزل عن التطور الذي يشكل ملمحاً لم يكتمل بعد، حيث يصعب تحديد آثاره وتداعياته بشكل شامل ونهائي حالياً ومستقبلاً[1]، ومع اتساع نطاق استخدام الفضاء الإلكتروني زادت الرغبة في السيطرة عليه باعتباره ميداناً جديداً للعلاقات والتفاعلات بين الدول وبين الفاعلين من غير الدول، وأصبح سلاحاً ذا حدين، فقد يتطور الخلاف السياسي بين دولتين إلى مواجهة عبر الفضاء الإلكتروني، وقد يتطور إلى إحداث أضرار مادية ضخمة وهو ما يمثل مكمن الخطورة الأكبر في درجة التأثير على الصراع الدولي، خاصة في الوقت الذي تسعى فيه جميع الدول إلى الحصول على المعلومة واقتحام أنظمة المعلومات السرية للأجهزة العسكرية والمعلوماتية، إلا أنه يلعب في الوقت نفسه دوراً في المساعدة على منع الصراعات، وذلك من خلال المساعدة في تقريب وجهات النظر وتبادل الأفكار والرؤي والآراء، حيث يشهد الفضاء الإلكتروني عبر الشبكات الاجتماعية والتجمعات الإلكترونية زيادة العلاقات بين المواطنين عبر الدول، وسهولة تبادل المعلومات والبيانات، والمساعدة في تجاوز الهياكل البيروقراطية للحكم، كما عزز الفضاء الإلكتروني من التغيير الهيكلي للدبلوماسية بالانتقال الجزئي من الاعتماد على الدولة الرسمية إلى تفاعل جهات وجماعات وأفراد داخل الدولة، والانتقال من مرحلة تبني النموذج المركزي في صنع السياسة الخارجية للانفتاح على طرق تنفيذ أهدافها، وتم تنشيط الاتصالات الداخلية ووزارة الخارجية والانفتاح على المعلومات.

ويأخذ الصراع الإلكتروني طابعاً تنافسياً حول الاستحواذ على سبق التقدم التكنولوجي وسرقة الأسرار الاقتصادية والعلمية إلى أن يمتد ذلك الصراع إلى محاولة السيطرة على الإنترنت من خلال السعي للسيطرة على أسماء النطاقات وعناوين

1- إيهاب عبدالحميد خليفة، **القوة الإلكترونية والصراع الدولي**، مقال منشور على موقع المركز العربي لأبحاث الفضاء الإلكتروني، بتاريخ 30 أغسطس 2013، يمكن المطالعة على:
http://www.accronline.com/print_article.aspx?id=15636

المواقع والتحكم بالمعلومات والعمل على اختراق الأمن القومي للدول من دون استخدام طائرات أو متفجرات أو حتى انتهاك الحدود السيادية كهجمات قرصنة الكمبيوتر وتدمير المواقع والتجسس بما يكون له من تأثير على تدمير الاقتصاد والبنية التحتية بنفس القوة التي قد يسببها تفجير تقليدي مدمر[1].

وللصراع الإلكتروني خصائص تميزه هي:

- الفاعلون الدوليون متنوعون وفي بعض الأحيان مجهولون.

- غير مكلف مادياً أو مالياً.

- سهولة البداية والانتهاء.

- به جزء مادي متمثل في خضوع الأجهزة والخوادم Servers والحاسبات لسلطان الدولة وسيادتها.

- قابلية تغيير خصائصها مستقبلاً نتيجة التغيرات السريعة في التكنولوجيا.

- الغالبية العظمى لا تستطيع نزع سلاح الطرف الآخر أو تدميره كلياً أو احتلال إقليمه.

- إمكانية استخدام الفضاء الإلكتروني في القوة الناعمة أو الصلبة.

ولما كان الصراع الإلكتروني أحد أوجه التفاعلات الدولية، فإنه يقابله أيضاً تحقيق الردع الإلكتروني، حتى تتمكن الدول من منع أي فاعل إلكتروني قادر على توظيف الإنترنت بصورة تخدم أهدافه من أن يتسبب في إلحاق الأذى بها، وتوصيل رسالة مفادها أن أي هجوم إلكتروني سوف يقابله هجوم مضاد قد يتسبب في خسائر فادحة للخصم، **ويتضح ذلك فيما يلي:**

1- عادل عبدالصادق، القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، **مرجع سابق،** ص 5.

ب- الردع الإلكتروني:

هدف الردع هو خلق مجموعة من المحفزات المانعة لقيام أحد أطراف الصراع من القيام باعتداء أو هجوم مستقبلاً[1]، وإذا كان ذلك هو هدف الردع في التفاعلات الدولية على أرض الواقع، فإنه مختلف جزئياً في حالة الردع الإلكتروني، لأن أحد الفواعل غير قادر على إزالة أو تدمير الطرف الآخر كلياً، كما في حالة الردع النووي مثلاً.

كما أنه ليس من السهولة تحقيق الردع الإلكتروني، بسبب خاصية التخفي، والتي تمنع مستخدم القوة الإلكترونية من التعرف على خصمه أو التوقع من أين سوف تأتيه الضربة، وهو ما يطرح سؤالاً حول إمكانية أن تقوم الهجمات الإلكترونية بتهديد السلم والأمن العالميين.

وفي ظل نظام دولي يتميز بتعدد القطبية، مما يزيد من احتمالات الصراع، فضلاً عن تعدد الفاعلين من الدول وغير الدول الذين يستخدمون القوة الإلكترونية في التفاعلات الدولية، بالإضافة إلى خاصية التخفي، فإن احتمالات الصراع الدولي تزداد.

ويتم ذلك من خلال القيام بهجمات إلكترونية على الشبكات العسكرية وسرقة معلومات استراتيجية أو الكشف عن الخطط والاستراتيجيات وقواعد البيانات الخاصة بالقوات المسلحة، وبالتالي تشكيل استراتيجيات مضادة، يدرك من خلالها الخصم أنه إذا قام بشن هجوم عبر الفضاء الإلكتروني سيواجه بهجوم آخر مضاد يفوق قدراته، كأن يتم مثلاً استهداف البنية التحتية الإلكترونية، أو أنظمة الاتصالات والأنظمة المالية والمصرفية، ومن ثم يرتدع الخصم عن محاولة التفكير في الاعتداء.

وتتنوع الوسائل التي تعتمد عليها الدول لردع أية محاولات للهجوم الإلكتروني وأهمها التجسس، ولم تعد تهم التجسس توجه فقط للولايات المتحدة والصين وروسيا، بل إن دائرة النطاق توسعت لتشمل عدة دول أوروبية، ومنها ما ذكرته مجلة "دير شبيغل" الألمانية في 17 أغسطس 2014، من أن الاستخبارات الألمانية

1- Martin C. Libicki, **Cyberdeterrence and Cyberwar**, (Santa Monica: RAND, 2009), P 28.

تجسست مرة على محادثات وزير الخارجية الأميركية، بينما تجسست على تركيا لعدة سنوات. ونُشرت معلومات حول قيام وكالة الأمن القومي الأمريكية بالتجسس على نحو 35 من القادة على مستوى العالم، وأكثر من 60 مليون مكالمة هاتفية في دول مختلفة، من بينها دول أوروبية[1]، وهي حادثة كشفت عن أن التجسس لم يعد يشمل قاطني الدولة، بل امتد إلى قاطني الدول الأخرى وقادتهم الذين هم بالأساس حلفاء مع الدولة، مما يزيد من عدم الثقة بين الحلفاء.

أما الوسيلة الأخرى فهي الحرمان من خدمات الإنترنت، أو قطع خدمات الإنترنت عن الدولة كاملة، ومثال على ذلك، انقطاع اتصالات الإنترنت في كوريا الشمالية لنحو عشر ساعات، مما أثار تكهنات بأن الولايات المتحدة وراء هذا الحدث، بسبب اتهام "بيونغ يانغ" بأنها وراء عملية القرصنة التي تعرضت لها شركة "سوني بيكتشرز" نهاية نوفمبر الماضي، خاصة أن الرئيس الأميركي باراك أوباما توعد بالرد.

ومن خلال تتبع بعض النماذج مثل الحرب بين روسيا وإستونيا عام 2007 وبين روسيا وجورجيا عام 2008، والاعتداء على البرنامج النووي الإيراني، واستخدام الفضاء الإلكتروني في عمليات التعبئة والتجنيد والحشد والحرب النفسية والإعلامية، نجد أن القوة الإلكترونية أصبحت تستخدم إلى جانب القوة العسكرية، بل أصبحت أحد المبادئ المهمة في أي استراتيجية عسكرية، مما جعل عملية التسلح الإلكتروني ذات أهمية بالنسبة لكثير من الدول، خاصة تلك التي تعتمد على الفضاء الإلكتروني بصورة أساسية.

1- NSA monitored calls of 35 world leaders after US official handed over contacts, **The Guardian,** On October 25, 2013.

ج- سباق التسلح على الفضاء الإلكتروني:

للتسليح أهمية استراتيجية مؤثرة في توازن القوى، وبسط النفوذ، وتمكين الدول من ممارسة العديد من الأدوار والضغوط والتكتلات في ظل بيئة أمنية يمتلكها الشك وعدم اليقين ومصالح استراتيجية قابلة للتدمير في ثوان معدودة، واتجهت الدول لتعزيز دفاعاتها ضد خطر التعرض للهجمات الإلكترونية، ولكن الاتجاه الأكثر خطورة هو التحول من اتخاذ إجراءات وقائية ذات طابع دفاعي إلى الاتجاه إلى تبني سياسات هجومية، وهو ما يحمل خطورة عسكرة الفضاء الإلكتروني دون الأخذ بعين الاعتبار كونه يختلف عن ظروف التقدم في امتلاك الأسلحة النووية أو البيولوجية ومن دون الأخذ في الاعتبار حجم التدمير المنتظر وقوعه حال التعرض لهجوم إلكتروني، وهو ما يمثل خطورة خاصة مع السعي لتطوير هذه الأسلحة ونشرها في ساعات.

وعلى الرغم من سرية النشاط المتعلق بالقدرات الإلكترونية، فإن التوقعات تشير إلى أن هناك ما لا يقل عن 120 دولة تقوم بتطوير طرق للتجسس واستخدام الإنترنت كسلاح لاستهداف أسواق المال ونظم الكمبيوتر الخاصة بالخدمات الحكومية، ومن أهم الدول التي تمتلك قدرات هجوم إلكترونية الولايات المتحدة والصين وروسيا وإسرائيل وفرنسا وبريطانيا والهند وألمانيا[1].

وقد دفع عجز حلف الناتو في مواجهة الهجمات الإلكترونية على إستونيا وجورجيا إلى تكوين وحدة للدفاع الإلكتروني مقرها تالين عاصمة إستونيا، وعمل على تطوير المفهوم الاستراتيجي للحلف، بحيث أصبح الفضاء الإلكتروني منطقة لعمليات الحلف، وأن عليه أن يطور قدراته الدفاعية الإلكترونية بما يشمل مساندة ودعم حلفائه الذين يتعرضون لهجمات إلكترونية، وأنه وفقاً لذلك فإن أي هجوم يتم على أوروبا أو أمريكا الشمالية يعتبر هجوماً ضد الجميع[2].

1-Misha Glenny, **The cyber arms race is on**, August 25, 2012
http://www.post-gazette.com/pg/11296/1183849-109-0.stm#ixzz1oMTYghXF

2- عادل عبدالصادق، القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، **مرجع سبق ذكره**، ص 13.

وإجمالاً، يمكن القول إن دولة ما تتمتع بقدرات إلكترونية متقدمة من خلال النظر إلى عدة متغيرات رئيسية منها:

- خطة استراتيجية خاصة برؤية الدولة لتعظيم قدرتها الإلكترونية.

- جهة مختصة بالدفاع عن الشبكة الإلكترونية للدولة وحمايتها والعمل على تطويرها.

- بنية تحتية تكنولوجية Cyber Infrastructure، مع الاهتمام بتطويرها وتحديثها بصفة مستمرة.

- شراكات مع القطاع العام والخاص لميكنة النظم والخدمات، وعمل استراتيجيات لتأمينها.

- قوانين تحافظ على الخصوصية، وتمنع ارتكاب الجرائم الإلكترونية.

- نظام تعليمي متقدم يدعم الابتكار ويعتمد على التكنولوجيا المتقدمة.

- عناصر بشرية متدربة وقادرة على استخدام التكنولوجيا الحديثة.

- تطوير أسلحة إلكترونية Cyber weapons تمكن الدولة من تحقيق أهدافها.

- قدرة الدولة على إدارة عمليات إلكترونية Computer Network (CNO) Operations تشمل مهاجمة شبكات الحاسب الآلي إذا دعت الحاجة إلى ذلك، والدفاع عن شبكاتها الخاصة، واستطلاع Exploitation الشبكات الأخرى.

الخلاصة:

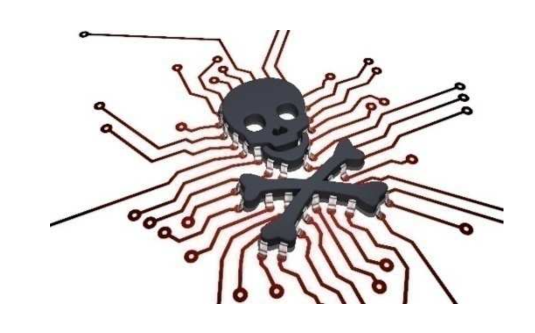
مما سبق نصل إلى نتيجة مفادها أن أشكال القوة تتغير بتغير التكنولوجيا، وقد ساهمت المميزات التي يتمتع بها الفضاء الإلكتروني من انخفاض في التكلفة وسهولة في الاستخدام وقدرة على التأثير في الآخرين، في تعدد استخداماته، سياسياً واقتصادياً وعسكرياً، فأثر على الأشكال التقليدية للقوة، وطرح مفهوم وشكل جديد هو القوة الإلكترونية، وقد كان لهذا الشكل الجديد دور في بلورة مفهوم انتشار القوة، حيث يتعدد الفاعلون الممارسون لها سواء من الدول أو من غير الدول، مما هدد الدور التقليدي للدول وقلل من سيادتها على إقليمها، ولم ينته الأمر عند ذلك، حيث ظهرت أشكال جديدة من الأسلحة، وعلى الرغم من ضآلة حجمها الذي لا يتعدى كيلوبايتس وقلة تكلفتها، إلا أنها تسبب خسائر فادحة على مختلف المستويات الاقتصادية والسياسية والعسكرية، بل وعلى المستوى الشخصي والفردي، فالضحية في هذه الحالة كل مشترك في خدمة الإنترنت، فالخسائر لا تعترف بالنوع ولا العمر ولا الإقليم، وبالتالي فمن الضروري وضع أطر حاكمة لاستخدامات هذه القوة وتقنينها بما يعمل على تحقيق الأمن الشخصي للمواطن، والأمن الدولي لمختلف الفواعل الدولية.

الفصل الثاني

أبعاد القوة الإلكترونية الأمريكية

إن الهدف الرئيسي لأي دولة من امتلاك القوة وتعظيمها هو العمل على حماية حدودها وأمنها وإقليمها ومصالحها من أي اعتداء، سواء داخلياً أو خارجياً، ومن ثم قد يتطلب الأمر الاستخدام المباشر لهذه القوة ليس مجرد رد اعتداء ولكن لمنع حدوث هذا الاعتداء أصلاً، ولما كانت القوة الإلكترونية إحدى الأدوات التي يمكن التعويل عليها في حماية أي تهديد للأمن القومي، كان من الضروري الوقوف على أبعاد القوة الإلكترونية للولايات المتحدة الأمريكية وحدودها، خاصة في ظل نظام دولي تآكلت فيه سيادة الدولة، ولا توجد به سلطة عليا أو حكومة عالمية تعمل على تنظيم مدخلاته ومخرجاته، أو مجموعة قواعد قانونية صارمة تحدد المسؤوليات والواجبات.

ومن ثم فإن هذا الفصل يسعى لاستعراض أبعاد القوة الإلكترونية الأمريكية في ضوء التهديدات الإلكترونية التي تواجه مصالح الولايات المتحدة الأمريكية في الفضاء الإلكتروني، بغرض استكشاف حدود القوة الإلكترونية الأمريكية ومعوقات استخدامها، ولذلك ينقسم هذا الفصل إلى ثلاثة مباحث، يتعرض أولها للمصالح والتهديدات التي تواجه الولايات المتحدة الأمريكية في الفضاء الإلكتروني، بينما يحلل المبحث الثاني عناصر القوة الإلكترونية الأمريكية من حيث العقيدة والاستراتيجية والبرامج والأدوات، أما المبحث الثالث فيتناول حدود القوة الإلكترونية الأمريكية ومعوقات استخدامها.



المبحث الأول

المصالح والتهديدات الأمنية التي تواجه الولايات المتحدة الأمريكية في الفضاء الإلكتروني

باتت مَيْكنة الأنظمة ومعظم أوجه الخدمات من معايير تقدم المؤسسات الحكومية، فيما يطلق عليه "الحكومة الإلكترونية"، بالإضافة إلى البورصات والمؤسسات المالية، فضلاً عن الشركات الخاصة، كنتيجة للتطور في جودة الشبكات وأنماط الاتصالات. وفي خِضم الانبهار بما وصل إليه التقدم التكنولوجي في هذا المجال، يغيب عن البعض مدى هشاشة تلك النظم التكنولوجية في مواجهة التطورات في مجالات القرصنة وصناعة الفيروسات، بحيث تصبح كفاءة المؤسسات الحكومية والخاصة رهن القدرات المتنامية لجماعات القرصنة الإلكترونية، وتواضع إمكانات المقاومة والحماية المتوفرة حتى الآن.

وفي الوقت نفسه أصبح الاقتصاد العالمي أكثر ترابطاً عبر الفضاء الإلكتروني، من خلال ملايين العمليات المالية والتجارية اليومية التي تتم من عبره، حيث دخل بكثافة في عمل العديد من المرافق الحيوية وأنظمة النقل والمواصلات والملاحة سواء في البر أو البحر أو الجو أو الفضاء الخارجي، وسرّع من عملية انتقال الأموال والاستثمارات والأفكار والأفراد، حيث تشير التقديرات إلى أن عدد مستخدمي الإنترنت في العالم قد بلغ 2.2 مليار شخص عام 2013، وهو ما يزيد من أهميته وخطورته في الوقت نفسه[1].

ولما كان الفضاء الإلكتروني أحد مصادر التهديدات التي تواجه الدولة، كان لابد من وضع عدة استراتيجيات وخطط للتعامل مع المخاطر التي يطرحها والتي قد تتسبب في تهديد الأمن القوي الأمريكي، حيث تكمن خطورة الفضاء الإلكتروني

1- Zia DaniellWigder, **Global Online Population Forecast, 2008 To 2013**, On September 10 th, 2013, on
http://www.forrester.com/Global+Online+Population+Forecast+2008+To+2013/fulltext/-/E-RES53355

وشبكات الكمبيوتر في اعتماد الولايات المتحدة عليها بشكل متزايد خاصة في أنظمة النقل والمواصلات ومحطات الطاقة والربط المالي والتجاري وأنظمة الدفاع والاتصالات، وهو الأمر الذي يعني أن تهديد إحدى هذه النظم أو القطاعات هو تهديد للأمن القومي الأمريكي، في الوقت ذاته للولايات المتحدة مصالح استراتيجية في الفضاء الإلكتروني تتعلق بالأمن القومي الأمريكي على مختلف المستويات السياسية والعسكرية وغيرها، وهو الأمر الذي يجعلها تسعى دائماً للسيطرة عليه، منذ بداية الإنترنت في معامل وزارة الدفاع الأمريكية، حينما عمدت الحكومة الأمريكية منذ عام 1998 إلى تطبيق منهج جديد لإدارة الإنترنت من خلال إنشاء كيان دولي لا يهدف للربح تحت سيطرتها، هذا الكيان الجديد هو هيئة الإنترنت لتنظيم الأسماء والأرقام التي تعرف اختصاراً باسم (آيكان ICANN)[1].

وقد تعرضت "آيكان" لضغوط شديدة للإصلاح من جانب دول مثل روسيا والصين وبعض الدول الأوروبية، والسبب الرئيسي هو رغبة الحكومات في التأثير بشكل أكبر على الإنترنت، حيث يعتبرون عمل الآيكان إنقاصاً لسيادتهم، خاصة بشأن الرقابة الأحادية على الإنترنت من جانب الولايات المتحدة من خلال الآيكان، مبررة ذلك بقولها إذا كان للحكومة الأمريكية هذه السلطة، لماذا لا يمكن للحكومات الأخرى الحصول عليها؟

ونتيجة لذلك شهدت أروقة الدورة الأولى للقمة العالمية لمجتمع المعلومات المنعقدة في جنيف عام 2003 جدلاً عنيفاً حول القضية، وضغوطاً من جانب منظمات المجتمع المدني وحكومات ومنظمات دولية عديدة اتفقت جميعها على ضرورة تغيير الوضع القائم، وعلى الرغم من ذلك باءت هذه الضغوط بالفشل، وتكرر نفس السيناريو قبيل قمة الأمم المتحدة لمجتمع المعلومات في نوفمبر 2005 بتونس، حيث انتقد ائتلاف من دول نامية ومتقدمة تحكم الولايات المتحدة الأحادي في نظام أسماء حقول الإنترنت (Internet's Domain Name System) من خلال منظمة

1- The Internet Corporation for Assigned Names and Numbers (ICANN) وهي هيئة دولية فنية بالأساس مقرها ولاية كاليفورنيا الأمريكية، تعني بتطوير الإنترنت، وقد نشأت هذه الهيئة بعد عملية مشاورات قادتها الحكومة الأمريكية مع عدد من الحكومات وخبراء في مجال الإنترنت، بهدف وضع عملية إدارة أسماء النطاقات وأرقام الإنترنت في إطار مؤسسي.

"الآيكان"، ومن ثم تم اقتراح إنشاء مجلس متعدد الجنسيات لمراقبة الشبكة، وهو الأمر الذي عارضته الولايات المتحدة للحفاظ على مصالحها في عالم الفضاء الإلكتروني وضمان سيطرتها عليه[1].

وعلى الرغم من ذلك جاءت ثمار هذا الجهد بتوقيع اتفاقية عام 2009 بين الآيكان ووزارة التجارة الأمريكية تدعم نموذج الرقابة الدولية للآيكان القائم على خضوع القرارات للإشراف الكلي للدول الأعضاء[2]، فضلاً عن ذلك لم تعد اللغة الإنجليزية هي اللغة الوحيدة المستخدمة لتسجيل نطاقات مواقع الإنترنت، حيث تلقت الآيكان في نوفمبر 2009 ما يقرب من تسعة عشر طلباً تمثل إحدى عشرة لغة مختلفة[3]، وفي عام 2010 منحت المنظمة الضوء الأخضر لمصر والسعودية والإمارات لتدوين عناوين مواقع الإنترنت باللغة العربية[4].

1- هل يستمر احتكار الولايات المتحدة لإدارة الإنترنت؟، **موقع BBC**، 15 نوفمبر 2005، بتاريخ مطالعة 11 سبتمبر 2013، يمكن المطالعة على الرابط التالي:

http://news.bbc.co.uk/hi/arabic/sci_tech/newsid_4440000/4440840.stm

2- اتفاق تاريخي يمنح منظمة الآيكان استقلالية كبري عن الحكومة الأمريكية، **موقع الأهرام الرقمي**، بتاريخ 13 أكتوبر 2009، بتاريخ مطالعة 11 سبتمبر 2013، يمكن المطالعة على :

http://digital.ahram.org.eg/articles.aspx?Serial=6937&eid=1297

3- باهر عصمت، الإنترنت ومنظمة الآيكان، **مجلة السياسة الدولية**، عدد أبريل 2010، (مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، أبريل 2010)، ص 64.

4- "الآيكان" تعطي الضوء الأخضر لتدوين عناوين مواقع الإنترنت باللغة العربية، **موقع فرنسا 24**،**بتاريخ 6 يونيو 2010**، تاريخ مطالعة 11 سبتمبر 2013، يمكن المطالعة على الرابط التالي:

http://www.france24.com/ar/20100506-multimedia-internet-icann-organisation-arabic-url-authorization-alphabetic-letter

11سبتمبر .. نقطة تحول في التهديدات الإلكترونية

قامت لجنة مشتركة من الحزبين الجمهوري والديمقراطي عام 2000 بدراسة ماهية المصالح القومية الأمريكية وقدمت تقريراً في هذا الشأن، قام بتعريف المصالح الحيوية للولايات المتحدة بأنها "تلك المتطلبات التي تجعل الولايات المتحدة قادرة على حماية وتدعيم وجودها، وأن تكون دولة حرة وآمنة"[1].

ثم جاءت إدارة الرئيسين بوش وأوباما لتضع العديد من الوثائق والاستراتيجيات التي حددت المصالح الأمريكية ومصادر التهديد لها، حيث يتمثل الإطار العام لهذه المصالح في الآتي[2]:

1- هزيمة الأعداء، وكسب المعارك والصراعات، وحماية أمن المواطنين الأمريكيين.

2- منع الأعداء من امتلاك أسلحة الدمار الشامل.

3- الاستعداد الدائم لأي تهديدات طارئة أو غير متوقعة ووضع خطط مستقبلية لمواجهتها.

وفي هذا السياق يعد الحادي عشر من سبتمبر 2001، بداية عهد جديد فيما يتعلق بالجوانب الأمنية، فمع انهيار برجي التجارة العالميين، انهارت معهما المفاهيم التقليدية للتهديدات الأمنية. وتغير سيناريو الحرب الباردة الذي هيمن على العالم على مدار أكثر من 50 عاماً بشكل جذري وحاسم، وظهر نوع جديد من التهديد العابر للحدود، فالحدود الإقليمية لم تعد ذات قيمة وكذلك القواعد العسكرية الخاصة بالمكان والزمان، وقد ينطبق هذا الوصف تماماً على التهديدات الإلكترونية،

1- Graham T. Allison, Dimitri K. Simes, James Thomson. Editors, **America's National Interests**, The Commission on America's National Interests, July 2000, p19.http://belfercenter.ksg.harvard.edu/files/amernatinter.pdf

2- Aki J. Peritz& Michael Sechrist,**Protecting Cyberspace and the US National Interest**, (Harvard Kennedy school, September 2010), p 3.

حيث تطورت تكنولوجيا المعلومات بشكل كبير، من أدوات إدارية لمساعدة تنفيذ العمليات المكتبية، إلى أن تصبح أداة استراتيجية للصناعة والإدارة والجيش. فقبل 11 سبتمبر، كانت تتم مناقشة المخاطر الإلكترونية والتحديات الأمنية في إطار مجموعات صغيرة من خبراء التقنية. لكن، منذ هذا التاريخ بات من الواضح أن عالم الإنترنت يحمل مواطن ضعف خطيرة للمجتمعات المترابطة بشكل متزايد.

وفي السياق ذاته جاءت أحداث إستونيا في صيف عام 2007 (عندما شنت روسيا هجمات إلكترونية ضد إستونيا على خلفية قيام الحكومة نصب تذكاري روسي من العاصمة تالين، لتجذب الانتباه السياسي لهذا التهديد المتزايد على الأمن العام واستقرار الدولة. وأثبتت موجات الهجمات الإلكترونية الخطيرة التي امتدت لثلاثة أسابيع أن مجتمعات الدول الأعضاء في (منظمة حلف شمال الأطلنطي) الذي تتزعمه الولايات المتحدة الأمريكية معرضة بشكل كبير للمخاطر على الجبهة الإلكترونية.

وهو الأمر الذي جعل الولايات المتحدة تجري سنوياً محاكاة للتعرض لحرب إلكترونية فيما يطلق عليه Cyber Storm أو عاصفة الحواسب، وفي الوقت نفسه خصصت مبلغ 500 مليون دولار في ميزانية 2012 لمواجهة هذه التهديدات الإلكترونية، وعملت على تطوير أسلحة إلكترونية تشمل فيروسات قادرة على تخريب شبكات العدو، كما ارتفع تمويل الأبحاث الخاصة بالحرب الإلكترونية من 120 مليون دولار إلى 208 ملايين دولار عام 2012[1].

1- عادل عبد الصادق، القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، **مرجع سابق**، ص 13.

وارتباطاً بما سبق يمكن القول إن أبرز الأهداف الإلكترونية التي يتم استهدافها في الولايات المتحدة الأمريكية تتمثل فيما يلي[1]:

- **على المستوى الاتحادي:** البيت الأبيض، الكونجرس الأمريكي، وزارة الداخلية، وذلك لأنها رموز للأمن القومي الأمريكي.

- **على المستوى العسكري:** يتم استهداف وزارة الدفاع والوحدات القيادية القتالية بهدف عرقلة العمليات العسكرية كما هي الحال في العراق وأفغانستان.

- **على المستوى المدني:** يتم استهداف البنية التحتية مثل المؤسسات المالية ومحطات الطاقة والاتصالات، وذلك لأنها تصيب أكبر عدد من المواطنين.

ويمكن تقسيم التهديدات الإلكترونية التي تواجهها الولايات المتحدة إلى الآتي:

هناك علاقة طردية موجبة بين زيادة الاعتماد على الفضاء الإلكتروني وبين التهديدات الإلكترونية، ولما كانت الولايات المتحدة تعتمد على الفضاء الإلكتروني بدرجة كبيرة، فكان أكثر عرضة للتهديدات الإلكترونية والتي كان منها سرقة بيانات ومعلومات اقتصادية وعسكرية وسياسية، وسرقة براءات الاختراع وحقوق الملكية الفكرية والتكنولوجيا المتطورة، وكذلك التلاعب بالبيانات المالية والاقتصادية وتزييفها أو اختراقها وسرقتها.

1-Kristin M. Lord And Travis Sharp, Editors, **America's Cyber Future: Security And Prosperity In The Information Age**, Volume2 (Center For A New America Security, June 2011). P 35.

أولاً: التهديدات الاقتصادية:

تعتبر الهجمات الإلكترونية ذات الطابع الاقتصادي من أخطر الهجمات التي يمكن أن تتعرض لها الولايات المتحدة، وذلك لأن النظم المالية والمصرفية والتجارية جميعها تعمل إلكترونياً، كما أن شركات التكنولوجيا العملاقة بما تحتويه أنظمتها الإلكترونية من براءات اختراع وحقوق ملكية فكريه ومشاريع تطوير سريه، هي عرضة للاختراق الإلكتروني وسرقة هذه المعلومات لصالح دول أو شركات منافسة، مما يعرض الاقتصاد الأمريكي لخسائر جمة، سواء نتيجة لسرقة معلومات اقتصادية وتجارية مهمة، أو سرقة براءات اختراع تضعف من قدرة المنتج الأمريكي على المنافسة في السوق الدولية.

وتعد الصين من أهم الدول التي قد تلحق بالولايات المتحدة خسائر اقتصادية بل وعسكرية عبر الفضاء الإلكتروني[1]، سواء من خلال سرقة البيانات الاقتصادية أو حقوق الملكية الفكرية وبراءات الاختراع، حيث إن الاعتداءات المستمرة على شبكات المعلومات ومحاولة اختراق بعض البيانات والمعلومات الحساسة والمهمة لدى الحكومة الأمريكية، خاصة بواسطة دول مثل الصين وروسيا، تجعل الولايات المتحدة عرضة لأي اختراق خارجي، ومن ثم تفقد ميزاتها النسبية من خلال سرقة البيانات والمعلومات الاقتصادية والعسكرية[2]، حيث فقدت الصناعة الأمريكية ما يقدر بـ 400 مليار دولار أمريكي بسبب سرقة المعلومات من خلال هجمات الكمبيوتر[3].

1-Jeffrey L. Caton**, Information As Power And America's National Security**, (U.S. ARMY WAR COLLEGE, May 2012), p 2.
2- Keeping the Nation's Industrial Base Safe From Cyber Threats, **Cyber Threats to National Security**, (Carnegie Institution for Science, Washington, D.C, September 2011), p 11.
3-Wilson Clay, **Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.**(CRS Reports. 29 January 2008). P 5-10.

ثانياً: التهديدات العسكرية:

وعلى الرغم من أن القوة الإلكترونية لم ترتق بعد لتتساوى مع القوة البحرية والجوية في حسم المعارك الحربية، فإن ميزتها النسبية تكمن في ربط الوحدات العسكرية بعضها ببعض بالأنظمة العسكرية الإلكترونية، بما يسمح بسهولة تبادل المعلومات وتدفقها، وسرعة إعطاء الأوامر العسكرية، والقدرة على إصابة الأهداف وتدميرها عن بعد مثلما يحدث من خلال الطائرات بدون طيار، أو أنظمة توجيه الأسلحة عن بعد. وقد تتحول هذه الميزة إلى نقطة ضعف، إن لم تكن الشبكة الإلكترونية المستخدمة في ذلك مؤمنة جيداً من أي اختراق خارجي، منعاً للتجسس أو التلاعب بالبيانات أو تدميرها أو التلاعب بالأنظمة العسكرية وإعادة توجيه أسلحة الخصم ضد أهداف وهمية أو صديقة، حيث يمكن سرقة تيرابايتس من المعلومات الدقيقة والحساسة والمتنوعة في دقائق معدودة، وهو ما حدث عندما تم تسريب ملايين الوثائق السرية من وزارة الخارجية الأمريكية عبر موقع الويكيلكس.

وقد انطلقت في عام 2008 واحدة من أخطر الهجمات ضد أنظمة حواسب الجيش الأمريكي. من خلال وصلة USB بسيطة متصلة بكمبيوتر محمول تابع للجيش في قاعدة عسكرية موجودة في الشرق الأوسط، ولم يتم اكتشاف انتشار برامج التجسس في كل من الأنظمة السرية وغير السرية في الوقت المناسب، مما شكل ما يشبه جسراً رقمياً، تم من خلاله نقل آلاف الملفات من البيانات إلى خوادم خارجية، ومنذ ذلك الحين، أصبح التجسس الإلكتروني يشكل تهديداً دائماً، وقد وقعت حوادث مماثلة في معظم دول حلف شمال الأطلنطي، غير أن أبرز هذه الحوادث قد وقع في الولايات المتحدة، حيث تم استهداف أكثر من 72 شركة من بينها 22 مكتباً حكومياً و13 من مقاولي قوات الدفاع[1].

1- الحرب الإلكترونية أخطر تهديد إيراني، **موقع CNN**، بتاريخ 7 نوفمبر 2013، بتاريخ دخول 10 سبتمبر 2014، يمكن المطالعة على:

http://archive.arabic.cnn.com/2012/scitech/11/6/_iran-cyberattack /

وفي السياق ذاته يمكن القول إن لم تكن هذه الحوادث تحمل التهديد الكافي، فإن التطور النوعي والكمي في القدرات المدمرة للحرب الإلكترونية أدى إلى مزيد من التهديدات الإلكترونية، فعلى سبيل المثال، أدى ظهور فيروس ستاكسنت الذي ظهر في عام 2010 إلى تحول من إصابة البعد المعلوماتي إلى إصابة المكون المادي نفسه، حيث أعلنت الاستخبارات الإيرانية أن هذا الفيروس أصاب ما يقدر بستة عشر ألف جهاز كمبيوتر، وتسبب في تعطيل آلاف أجهزة الطرد المركزي بالبرنامج النووي الإيراني، وقد تبنت إسرائيل المسؤولية عن شن هجمات ستاكسنت بالتعاون مع الولايات المتحدة للعمل على تعطيل المنشآت النووية كجزء من منصة لإطلاق الفيروسات الخطرة تم تطويرها عام 2007 وتمت تجربتها في إسرائيل، وكان هذا بمنزلة دليل على أن الهجمات الإلكترونية يمكنها أن تسبب أضرار مادية حقيقية وتهدد حياة البشر[1]. هذا فضلاً عن الهجمات العسكرية التي تستهدف تدمير بعض الخوادم أو الكابلات والألياف الضوئية أو تدمير الأقمار الصناعية وشبكات الكمبيوتر باستخدام الأسلحة التقليدية، مما يتسبب في شل سبل الحياة الإلكترونية.

1- التهديدات الجديدة: الأبعاد الإلكترونية، **مجلة حلف الناتو**، تاريخ المطالعة 6 سبتمبر 2012، يمكن المطالعة على الرابط التالي:

http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/AR/index.htm

ثالثاً: الإرهاب الإلكتروني:

يُعد الإرهاب الإلكتروني مثله مثل أي اعتداء من قراصنة هدفهم التخريب أو سرقة البيانات، ولكن الهدف في الأساس سياسي، ويسعى للإضرار بالأمن القومي للدولة وليس الحصول على بعض المكاسب الشخصية بصورة غير شرعية أو مجرد جذب الانتباه.

حيث يمكن استخدام الفضاء الإلكتروني في العمليات الإرهابية من خلال:

1- التجنيد والتعبئة والدعاية والإعلان وجمع التمويل.

2- التواصل والتخطيط وإدارة الاجتماعات وجمع المعلومات وإرسالها.

3- تقديم الوصفات الجاهزة لصناعة القنابل والمُفرقعات.

4- مهاجمة نُظم التحكم في الطيران لإحداث تصادم سواء بين الطائرات، أو قطارات السكك الحديديَّة.

5- تعطيل البنوك وعمليَّات التحويل المالي، مما يُلحق الأذى بالاستثمار والاقتصاد الوطني.

6- تعديل ضغط الغاز عن بعد في أنابيب الغاز لتفجيرها.

7- التلاعب في نظم السلامة في المصانع الكيماوية لإحداث أضرار بالمواطنين.

8- الدخول عن بُعد لنظام التحكُّم في علاج المرضى في المستشفيات بهدف قتل المرضي، وفي مصانع غذاء الأطفال لتغيير مُستويات نسب المواد الغذائيَّة بهدف قتل الأطفال.

9- التحكم في أنظمة المواصلات خاصة على الطرق السريعة والأنفاق والكباري لإحداث إرباك مروري أو حوادث طرق.

10- السيطرة على أنظمة التحكم في السدود وقناطر المياه على الأنهار مما يسبب كوارث إنسانية.

11- السيطرة على شبكات الربط الكهربائي المتصلة بالإنترنت عبر أنظمة (SCADA)

رابعاً: تهديد البنى التحتية:

وتعتبر من أخطر الأهداف التي يمكن أن تشملها الهجمات الإلكترونية، لما قد يترتب عليها من خسائر فادحة، لأنها لا تقتصر فقط على الاستخدامات المدنية لها بل والاستخدامات العسكرية، وتشمل تهديد مختلف المصالح الحيوية للدولة.

ويمكن تعريف البنية التحتية الحرجة للولايات المتحدة بأنها عبارة عن: النظم والأصول سواء كانت مادية أو افتراضية Virtual، والتي يتسبب تدميرها أو التلاعب بها في تهديد الأمن القومي الأمريكي أو الاقتصاد الوطني أو الرعاية الصحية أو الأمن العام[1].

ويمكن التمييز بين ثلاثة أنوع من البنى التحتية هي:

أ- الأصول المادية: سواء كانت مادية، مثل الأصول الثابتة والعقارات والمنتجات أو غير مادية كالمعلومات.

ب- القوى البشرية: خاصة تلك المتعاملة مع نظم الكمبيوتر والمعلومات والتي يمكن اختراقهم أو اختراق الأنظمة التي يعملون عليها.

ج- الأصول الإلكترونية: والتي تشمل أجهزة الكمبيوتر والخوادم والشبكات والأنظمة الإلكترونية والبرامجية.

وقد حددت الاستراتيجية القومية الأمريكية للأمن الداخلي لعام 2006 عدد 12 عنصراً من عناصر البنية التحتية الحرجة بالنسبة للولايات المتحدة الأمريكية تتمثل في: الاتصالات السلكية واللاسلكية، ومحطات الطاقة والكهرباء، والبنية التحتية الخاصة بصناعة نظم الدفاع والأسلحة، ونظم استخراج وصناعة ونقل وتخزين الغاز والنفط، ونظم الزراعة وصناعة وتوزيع الأطعمة، والخدمات المصرفية والمالية، وشبكة

1-**Critical Infrastructure: Threats and Terrorism**, (US Army Training and Doctrine Command, August 2006). P I-1.

المواصلات، وإمدادات المياه من خزانات وسدود وقناطر، والخدمات الطبية، وخدمات البريد والنقل وخدمات الطوارئ مثل الإنقاذ والإسعاف والحرائق، وأخيراً الحكومة نفسها، حيث تم اعتبارها أحد هذه البنى التحتية بما تملكه من قدر على التحكم والرد المباشر على أي اعتداء أو هجوم[1]، ونتيجة لاعتماد هذه البنى على التكنولوجيا المتقدمة وخدمات الكمبيوتر فإنها تصبح في مرمى الهجمات الإلكترونية.

وقد حذر الاتحاد الدولي للاتصالات اللاسلكية من خطورة التهديدات التي تواجه الاتصالات، سواء كانت مادية أو إلكترونية، كما يعتبر فيروس ستاكسنتوفليم من أبرز الأسلحة الإلكترونية التي يتم استخدامها لتدمير بعض المكونات الصناعية وأنظمة الإدارة والتحكم[2]. ومن ناحية أخرى أوصت لجنة المصالح القومية الأمريكية بضرورة حماية البنية التحتية الأمريكية من الهجمات الإلكترونية، واعتبرت استراتيجية الأمن القومي الأمريكية الصادرة في مايو 2010 أن البنية التحتية الإلكترونية هي بمنزلة أصل قومي يجب تأمينه وحمايته لتدعيم الأمن القومي.

1-Ibid, pp II-1: II-10.
2-NazliChoucri, **Cyberpolitics in International Relations**, (The MIT Press Cambridge, Massachusetts London, England, 2012), P 151.

خامساً: التلاعب بالبيانات الشخصية وتهديد أمن المواطنين:

نتيجة لسهولة ورخص تكلفة الدخول إلى الفضاء الإلكتروني وزيادة عدد مستخدميه بصورة يومية، وإمكانية الدخول عليه من مختلف الوسائل التكنولوجيا بداية من جهاز الكمبيوتر المنزلي، مروراً بالهاتف المحمول والأجهزة اللوحية Tablets نهاية بالخوادم اللاسلكية التي تعتمد على شبكات التليفون المحمول USB Modems، فإن جميع الأفراد أصبحوا عرضة للهجمات الإلكترونية والتلاعب ببياناتهم الشخصية وسرقتها وانتحال شخصياتهم وأسمائهم.

كما تقوم الشركات الكبرى والمؤسسات التي تخدم الجمهور بحفظ قواعد البيانات الخاصة بالمواطنين على أجهزة كمبيوتر وخوادم، وتتم عملية الربط بينهم عبر شبكات الانترنت، وهو ما يعرضها لخطر القرصنة وسرقة البيانات والتلاعب بها وإساءة استخدامها، خاصة ما إذا كان الأمر يتعلق بالمسائل المالية والحسابات البنكية، فعلى سبيل المثال قام في سبتمبر 2004 بعض القراصنة باختراق أنظمة الكمبيوتر الخاصة بشركة تشويس بوينت ChoicePoint Inc التي تعمل في مجال الائتمان وجمع المعلومات الشخصية للمستهلكين، واستطاع القراصنة اختراق بيانات 163 ألف مشترك، وتمت سرقة بيانات 5000 حالة بالفعل[1].

1- Kristin M. Lord And Travis Sharp, **Op. Cit**, p 36.

ولمواجهة هذه المخاطر قامت الولايات المتحدة بوضع العديد من الخطط والاستراتيجيات التي تسعى إلى تحقيق الأمن الإلكتروني من خلال التالي:

1- التحرك نحو إدارة شبكة فيدرالية واحدة.

2- نشر أنظمة التحري والكشف عن الهوية.

3- تطوير ونشر أدوات منع الاختراق.

4- إعادة توجيه مجالات البحوث وإعادة النظر في تمويلها.

5- الربط الشبكي لمراكز العمليات الإلكترونية للحكومة الاتحادية.

6- تطوير خطة حكومية قائمة على مخابرات إلكترونية واسعة.

7- زيادة أمن الشبكات السرية.

8- توسيع نطاق التعليم الإلكتروني.

9- تحديد التكنولوجيات المستقبلية التي تجعل الولايات المتحدة متقدمة عن غيرها.

10- تحديد الأدوات التكنولوجيا والبرامجية التي تدعم عملية الردع الإلكتروني.

11- وضع مناهج متعدد الجوانب لزيادة كفاءة عملية إدارة المخاطر.

12- تحديد دور الأمن الإلكتروني في مجالات القطاع الخاص.

سادساً: تسريب البيانات المتعلقة بالأمن القومي الأمريكي:

يُعد تسريب البيانات أحد التهديدات الرئيسية التي تواجه الأمن القومي الأمريكي، خاصة البيانات الخاصة بالأمن القومي الأمريكي والتي تتعلق بالخطط التجارية والاستراتيجيات الاقتصادية وخطط التسلح والتطوير العسكري، وحقوق الملكية الفكرية وبراءات الاختراع، فضلاً عن المراسلات السرية بين الحكومة الأمريكية وموظفيها وعملائها داخل وخارج الولايات المتحدة، ولعل أبرز الأمثلة على ذلك هو قيام إدوارد سنودن الموظف السابق في وكالة الاستخبارات الأمريكية والمتعاقد مع وكالة الأمن القومي الأمريكي بعدما اتجه للقطاع الخاص[1]، وقبله جوليان أسانج مؤسس موقع الويكيلكس، بنشر ملايين الوثائق المصنفة على أنها سرية للغاية وتتعلق بالأمن القومي الأمريكي.

وكان أسانج قرصاناً إلكترونياً (هاكر)عندما كان مراهقا، ثم مبرمج الكمبيوتر، وبدأ في عام2009 بنشر وثائق عسكرية ودبلوماسية خاصة بالحكومة الأمريكية عبر موقع الويكيليكس، بمساعدة من أحد الضباط في الجيش الأمريكي هو "برادلي مانينغ" الذي حكمت عليه محكمة عسكرية أمريكية بالسجن لمدة 35 عاماً[2]، على

1- الاستخبارات الأميركية تخشى وجود إدوارد سنودن آخر في صفوفها، **موقع جريدة الحياة**، بتاريخ دخول 20 أغسطس، 2014، يمكن المطالعة على:
http://alhayat.com/Articles/3992870/%D8%A7%D9%84%D8%A5%D8%B3%D8%AA%D8%AE%D8%A8%D8%A7%D8%B1%D8%A7%D8%AA-%D8%A7%D9%84%D8%A3%D9%85%D9%8A%D8%B1%D9%83%D9%8A%D8%A9-%D8%AA%D8%AE%D8%B4%D9%89-%D9%88%D8%AC%D9%88%D8%AF-%D8%A5%D8%AF%D9%88%D8%A7%D8%B1%D8%AF-%D8%B3%D9%86%D9%88%D8%AF%D9%86-%D8%A2%D8%AE%D8%B1-%D9%81%D9%8A-%D8%B5%D9%81%D9%88%D9%81%D9%87%D8%A7

2- الحكم بالسجن 35 عاما على الجندي الأمريكي برادلي مانينغ في قضية "ويكيليس"، **موقع فرنسا 24**، بتاريخ 21 أغسطس 2013، بتاريخ دخول 20 أغسطس 2014، يمكن المطالعة على:
http://www.france24.com/ar/20130821-%D9%85%D8%AD%D9%83%D9%85%D8%A9-%D8%B9%D8%B3%D9%83%D8%B1%D9%8A%D8%A9-%D8%A8%D8%B1%D8%A7%D8%AF%D9%84%D9%8A-%D9%85%D8%A7%D9%86%D9%8A%D9%86%D8%BA-%D8%AC%D9%86%D8%AF%D9%8A-%D8%A3%D9%85%D8%B1%D9%8A%D9%83%D8%A7-%D8%AA%D8%B3%D8%B1%D9%8A%D8%A8-%D9%88%D8%AB%D8%A7%D8%A6%D9%82-

خلفية مساعدته لاسانج، وأعقبه قيام أدوردسنودن بتسريب برامج، خاصة بوكالة الأمن القومي الأمريكي عام 2013، تشير إلى قيام الولايات المتحدة بالتجسس على العديد من المواطنين داخل وخارج الولايات المتحدة، بل والتجسس على بعض الرؤساء والقادة السياسيين[1]، وهو ما يجعل الحفاظ على سرية البيانات، خاصة تلك المتعلقة بالأمن القومي الأمريكي تحدي رئيسي للحكومات الأمريكية، ومصدر تهديد إلكتروني.

%D8%B3%D8%B1%D9%8A%D8%A9-
%D9%88%D9%8A%D9%83%D9%84%D9%8A%D9%83%D8%B3/

1- Gellman, Barton; Markon, **Edward Snowden says motive behind leaks was to expose 'surveillance state**, The Washington Post**, June 10, 2013,** Accessed on August 20th, 2014,http://www.washingtonpost.com/politics/edward-snowden-says-motive-behind-leaks-was-to-expose-surveillance-state/2013/06/09/aa3f0804-d13b-11e2-a73e-826d299ff459_story.html?tid=pm_politics_pop

الخلاصة:

لاحظ الكاتب تغيراً في طبيعة التهديدات التي تستهدف الأمن الإلكتروني الأمريكي، والتي تحولت- خلال فترة الدراسة - من السعي لغلق أو شل المواقع الرسمية كثيرة الجمهور، مثل موقع البنتاجون أو الكونجرس أو البيت الأبيض، أو غلق المواقع الاقتصادية كالبنوك والمؤسسات التجارية، إلى نوع آخر من التهديدات الأكثر خطورة، تتعلق بسرقة بيانات ومعلومات اقتصادية وعسكرية وسياسية، وسرقة براءات الاختراع وحقوق الملكية الفكرية والتكنولوجيا المتطورة، وكذلك الإضرار بالأمن القومي الأمريكي من خلال التلاعب ببيانات المؤسسات المالية والاقتصادية وتزييفها أو اختراقها وسرقتها، أو الدخول إلى الشبكة القومية للكهرباء وإمكانية السيطرة عليها وشل قدراتها، وهو ما يعرض الأمن القومي الأمريكي لمخاطر جمة. كما أن هناك علاقة طردية موجبة بين زيادة الاعتماد على الفضاء الإلكتروني وبين التهديدات الإلكترونية، ولما كان المجتمع الأمريكي يتجه نحو المزيد من الاعتماد على الفضاء الإلكتروني أكثر من الطرق التقليدية كالتسوق مثلاً الذي يزداد بصورة ملاحظة عبر الإنترنت، وبعض المبادرات التي تستخدم الإنترنت كالتطبيب والعلاج عن بعد وغيرها، فإن من شأن ذلك زيادة المخاطر التي يواجهها المجتمع الأمريكي، خاصة في ظل اتجاه الدولة الأمريكية نحو توظيف الفضاء الإلكتروني في كافة المجالات، سواء كانت مالية أو تجارية أو صناعية أو أمنية أو تكنولوجيا أو ثقافية أو سياسية أو عسكرية، بحيث يمكن القول إن الولايات المتحدة قد أنشأت لها كياناً جديداً على إقليم جديد هو الفضاء الإلكتروني.

المبحث الثاني

عناصر القوة الإلكترونية الأمريكية خلال رئاستي بوش وأوباما: العقيدة، الاستراتيجية، البرامج، والأدوات

باتت قضية الأمن الإلكتروني تُشكل هاجساً متزايداً لدى دوائر صنع القرار الأمريكي وداخل الأروقة البحثية الأمريكية منذ أن تعرضت الولايات المتحدة لهجمات الحادي عشر من سبتمبر، وتزايد الاهتمام بقضايا الأمن الإلكتروني مع تزايد الاعتماد عليه في مختلف المجالات، وكان نتيجة لتعرض مصالح وهيئات حكومية أمريكية كبرى لضربات إلكترونية موجعة في مقدمتها وزارات الدفاع والخارجية والأمن القومي والتجارة، بالإضافة إلى وكالة الفضاء الأمريكية "ناسا" وجامعة الدفاع الوطني .National Defense University أثر مهم في وضع استراتيجيات خاصة بالأمن الإلكتروني الأمريكي، وهو ما خلق حالة من شبه الإجماع بين جميع الأوساط السياسية والعسكرية والاقتصادية إزاء ضرورة التصدي لهذا الخطر، مع وجوب تولي الحكومة الاتحادية الأميركية هذا الأمر، حيث أشارت تقارير صادرة من المكاتب الفيدرالية إلى زيادة الهجمات الإلكترونية التي تتعرض لها شبكات الكمبيوتر الخاصة بالحكومة الأمريكية، سواء من فواعل معروفة للحكومة أو غير معروفة، مما دعا المؤسسات الرسمية وغير الرسمية الأمريكية إلى وصف الأمن الإلكتروني بأنه قضية أمن قومي ملحة[1].

ويهدف هذا المبحث إلى تحليل مضمون الاستراتيجيات والوثائق والبرامج التي تحكم العقيدة الأمريكية في تعاملها مع التهديدات الإلكترونية خلال فترتي الرئيس بوش وفترة الرئيس أوباما الأولى.

1- James A. Lewis, **Securing Cyberspace for the 44the Presidency: A Report of the CSIS Commission on Cybersecurity for the 44the Presidency**, (Center for Strategic and International Studies, December 2008), p 11.

وقبل الحديث عن العقيدة والاستراتيجية نتطرق إلى موضع ومكانة القوة الإلكترونية الأمريكية وفقاً لمؤشر القوة الإلكترونية Cyber Power Index الصادر في عام 2013، عن وحدة التحليل الاقتصادي بمجلة الإيكونيميست الاقتصادية،والذي يهتم بقياس القوة الإلكترونية لمجموعة دول العشرين، ويتكون من 4 محددات رئيسية، هي الإطار التشريعي والحاكم لاستخدام القوة الإلكترونية، الإطار الاقتصادي والاجتماعي، البنية التحتية التكنولوجية، والتطبيقات الاقتصادية، وكل محدد منهم يتكون من مجموعة من الأوزان النسبية التي أعدها مجموعة خبراء، والتي استند إليها مؤشر القوة الإلكترونية، وقد حلت الولايات المتحدة في المرتبة الثانية بعد المملكة المتحدة بمجموع نقاط وصل إلى 75.4 من أصل 100 نقطة[1].

وبحسب المؤشر أيضاً فإن عناصر القوة الإلكترونية الأمريكية تمثلت في وجود استراتيجية لحماية النظم الإلكترونية، وحماية حقوق الملكية الفكرية، والتزام بتطوير تكنولوجيا الفضاء الإلكتروني، ووجود رقابة صارمة عليه، مع تطوير مستويات التعليم، والإنفاق المالي على تكنولوجيا المعلومات، والقدرة على تحمل أعباء هذه النفقات، ووجود خوادم مؤمنة من الاختراقات الإلكترونية، بالإضافة إلى وجود حكومة إلكترونية قوية، وتجارة إلكترونية أمريكية نشطة، مما يضعها في مرتبة متقدمة بين مجموعة دول العشرين فيما يتعلق بالقوة الإلكترونية[2].

1- **Cyber Power Index**, Economist Intelligence Unit, Accessed date August 2014, on http://www.boozallen.com/content/dam/boozallen/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf.

2 - Ibid.

وفيما يلي نتطرق إلى العقيدة الأمريكية خلال فترتي بوش وأوباما من حيث الخطط والاستراتيجيات والبرامج:

ساهمت تسريبات إدوارد سنودن في كشف العديد من برامج التجسس السرية الأمريكية، سواء على مواطنيها، أو على مواطني دول أخرى، سواء كانت حليفاً أو عدواً للولايات المتحدة، وقد نظرت إدارة الرئيس بوش إلى الفضاء الإلكتروني باعتباره أحد مصادر التهديد التي يمكن أن تستخدمه الجماعات الإرهابية كوسيط في تنفيذ عمليات عسكرية ضد الولايات المتحدة،بينما نظرت إدارة الرئيس أوباما إلى الفضاء الإلكتروني باعتباره أحد مصادر الرخاء والتقدم الاقتصادي.

أولاً: القوة إلكترونية في إطار إدارة الرئيس بوش الابن:

كان لأحداث الحادي عشر من سبتمبر 2001 أثر واضح على ممارسة القوة في العلاقات الدولية بصفة عامة، وتغير طبيعة الهيمنة والنفوذ في المجتمع الدولي بصفة خاصة، حيث أصبح بإمكان فواعل دون مستوى الدول أو عابرة لها التأثير في العلاقات الدولية، وبدلاً من الاعتماد كليةً على القدرات العسكرية، اعتمدت بصورة أكبر على القدرات الاقتصادية والتكنولوجية، وبرزت على الساحة الدولية جماعات وأطراف من غير الدول، كالجماعات الإرهابية ومنظمات المجتمع المدني والشركات متعددة الجنسية وأصبحت هناك قيود على قدرة الدولة على صنع السياسة الخارجية بل لم تعد الفاعل الأوحد في العلاقات الدولية، وأثرت الثورة المعلوماتية على إعادة توزيع وتغيير الأوزان النسبية للفاعلين في النظام الدولي، أو بمعنى آخر انتشار القوة في النظام الدولي.

وقد دفعت هذه الظروف الإدارة الأمريكية إلى اتخاذ إجراءات غير تقليدية، فقامت باستحداث وزارة الأمن الداخلي التي تم إنشاؤها في نوفمبر 2002، وما أعقبها من إصدار قانون الأمن الوطني (الباتريوت أكت)[1]، وأصدرت العديد من الاستراتيجيات

1-ElihuZimet and Edward Skoudis, A Graphical Introduction to the Structural Elements of Cyberspace, Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz Editors, **Cyber**

والوثائق التي تسعى لإعادة تعريف المخاطر والتهديدات التي تواجهها الولايات المتحدة، وكان أحد أهم هذه المخاطر هو التهديدات الإلكترونية القادمة عبر الفضاء الإلكتروني.

فمنذ بداية الحرب على الإرهاب تعرضت الولايات المتحدة الأمريكية للعديد من الهجمات الإلكترونية ذات المستوى العالي[1]، مما دفع الإدارة الأمريكية إلى وضع مجموعة من الخطط والاستراتيجيات والمبادرات والبرامج التي من شأنها تدعيم الأمن الإلكتروني الأمريكي، مثل الاستراتيجية القومية للحماية المادية للبنية التحتية الحرجة والأصول الرئيسية National Strategy For The Physical Protection Of Critical Infrastructures And Key Assets، والاستراتيجية القومية لتأمين الفضاء الإلكتروني National Strategy To Secure Cyberspace، والاستراتيجية القومية العسكرية للعمليات في الفضاء الإلكترونية The National Military Strategy For Cyberspace Operations، وكذلك المبادرة الوطنية الشاملة للأمن الإلكتروني Comprehensive National Cybersecurity Initiative, CNCI، ونصت الاستراتيجية القومية العسكرية عام 2004 على أن: القوات المسلحة يجب أن تكون لها القدرة على الحركة في الهواء والأرض والبحر والفضاء الخارجي والفضاء الإلكتروني الخاصة بالمعركة[2]، كما سمح قانون الأمن الوطني لسلطات الأمن بالحصول على تسجيلات الاتصالات التي تتم عبر البريد الإلكتروني من الشركات التي تقدم خدمات الإنترنت. وتم إنشاء المجلس الاستشاري الوطني للبنية التحتية The National InfrastructureAdvisory Council بهدف تحسين التعاون في مجال الأمن الإلكتروني بين البنوك والشركات والمصنعين والحكومات المحلية[3]،

Power and National Security, (Center for Technology and National Security Policy, Washington, D.C., 2009) p86.

1-**The Evolution of U.S. Cyberpower**,p 28 On http://www.afcea.org/committees/cyber/documents/TheEvolutionofUSCyberpower.pdfOn Oct 25th, 2013.

2- **The National Military Strategy of the United States of America**, (The White House, 2004), p1.

3-Timothy L. Thomas, Nation-state Cyber Strategies: Examples from China and Russia, Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz Editors, **Cyber Power and National Security**, (Center for Technology and National Security Policy, Washington, D.C., 2009) p434.

وفيما يلي عرض لأبرز ما تناولته هذه الاستراتيجيات الأمريكية في مجال التهديدات الإلكترونية:

أ- الاستراتيجية القومية للحماية المادية للبنية التحتية الحرجة والأصول الرئيسية

National Strategy For The Physical Protection Of Critical Infrastructures And Key Assets

وقع الرئيس بوش الابن على الاستراتيجية القومية للحماية المادية للبنية التحتية الحرجة NSPPCIKA في فبراير 2003 وقد ركزت هذه الاستراتيجية تحديداً على حماية البنية التحتية من الهجمات الإرهابية أكثر من الحماية من بشكل عام، وقد رسمت مستويات التعاون بين المؤسسات الحكومية وبعضها البعض. كما وضعت بعض الخطوات التي يجب على المواطنين والمؤسسات الرسمية وغير الرسمية أن تتخذها من أجل تدعيم الأمن الإلكتروني[1]، وتسعى هذه الاستراتيجية إلى تحقيق هدف رئيسي هو: **ضمان الحماية الكاملة للبنية التحتية الحرجة والأصول الرئيسية التي تؤثر على المستوى الوطني، مثل الصحة العامة والأمن العام والاقتصاد والأمن الوطني والثقة العامة لدى المواطنين**، مع تقديم إنذار مسبق في حالة تعرض هذه البنى لأي مخاطر أو تهديدات، بالإضافة إلى توفير الحماية للبنى التحتية الأخرى التي تكون بمنزلة أهداف رئيسية للإرهابيين من خلال تحفيز التعاون بين المؤسسات الرسمية وغير الرسمية لضمان توفير حماية أفضل لها[2].

وتؤكد الاستراتيجية على أن مفاهيم الأمن القومي قد تغيرت، وتغيرت أيضاً مصادر التهديد، فلم تعد هي مسؤولية الحكومة الفيدرالية فقط، خاصة فيما يتعلق بالحفاظ على البنى التحتية، حيث يشاركها أيضاً الحكومة المحلية والقطاع الخاص

1-Edward Skoudis, Evolutionary Trends in Cyberspace, Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz Editors, **Cyber Power and National Security**, (Center for Technology and National Security Policy, Washington, D.C., 2009) p 132.
2-**The National Strategy For The Physical Protection of Critical Infrastructures and Key Assets**, (The White House, February 2003) , P Vii..

والمواطنون، ولتحقيق هذا الهدف يجب فهم دوافع أعداء الولايات المتحدة والخطط والتكتيكات التي يتبعونها، ويجب استكمال هذا الفهم بعمل تقييم شامل للبنية التحتية التي يجب حمايتها ومواطن الضعف فيها.

وتحكم هذه الاستراتيجية ثمانية مبادئ رئيسية هي[1]:

1- ضمان سلامة الأمن العام والثقة العامة لدى المواطنين وأمن الخدمات العامة.

2- إرساء مبدأ المسؤولية والمحاسبة.

3- تشجيع وتسهيل الشراكة بين جميع المستويات الحكومية وقطاع الصناعات.

4- تشجيع حلول السوق كلما كان ذلك ممكناً وتعويض إخفاقات السوق بالتدخل الحكومي.

5- تسهيل تبادل المعلومات المفيدة.

6- تسريع عملية التعاون بين الولايات المتحدة والمجتمع الدولي.

7- تطوير التكنولوجيات والخبرات لمكافحة التهديدات الإرهابية.

8- حماية الخصوصية والحريات الدستورية.

1- Ibid, P 11-13.

ب- الاستراتيجية القومية لتأمين الفضاء الإلكتروني

National Strategy To Secure Cyberspace :

أطلق الرئيس بوش الابن الاستراتيجية القومية لتأمين الفضاء الإلكتروني في فبراير 2003، والتي تضمن الجهود اللازمة لتقليل المخاطر والتهديدات الناجمة عن الفضاء الإلكتروني، والتي من شأنها تدمير الأنظمة الخاصة بالبنية التحتية الأمريكية[1].

وقد تمت الإشارة في الاستراتيجية القومية لتأمين الفضاء الإلكتروني إلى أن البنية التحتية الأمريكية تتكون من مؤسسات عامة، خاصة في مجالات: الأغذية والزراعة والمياه والصحة العامة والطوارئ والدفاع والخدمات الحكومية والاتصالات والمعلومات والطاقة والنقل والصرافة والمعاملات المالية والبريد والملاحة والصناعات الكيميائية، ويعتبر الفضاء الإلكتروني عصب هذه المجالات، فهو نظام التحكم الخاص بالدولة، ومن ثم فتأمينه والقدرة على التحكم فيه وإدارته من العوامل الرئيسية للاقتصاد والأمن القومي الأمريكي، وهذا لن يتحقق إلا بوجود شراكة وتعاون مع القطاع الخاص.

وتسعى الاستراتيجية إلى تحقيق ثلاثة أهداف رئيسية هي[2]:

- منع الهجمات الإلكترونية.

- تقليل نقاط الضعف التي يمكن اختراقها.

- سرعة التعامل مع الهجمات الإلكترونية لتقليل إمكانية تدمير الأنظمة والبيانات والعمل على سرعة استعادتها. **ويمكن تحقيق ذلك من خلال**[3]:

1-Gregory J. Rattray , An Environmental Approach to Understanding Cyberpower, Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz Editors, **Cyber Power and National Security**, (Center for Technology and National Security Policy, Washington, D.C., 2009) p 254.
2- **The National strategy to secure cyberspace**, (The White House, 2003) p Viii.
3- Ibid, p X.

1- نظام وطني يقوم بتنسيق الجهود المشتركة لسرعة التعامل مع الهجمات الإلكترونية والحفاظ على البيانات.

2- برنامج قومي يهدف لتقليل المخاطر في الأنظمة الإلكترونية والحد من مواطن الضعف فيها.

3- برنامج قومي للتوعية والتدريب على أمن الفضاء الإلكتروني.

4- تأمين المؤسسات الحكومية ضد الهجمات الإلكترونية.

5- تدعيم التعاون الدولي في مجال الأمن الإلكتروني.

ومن الملحوظ أن العنصر الأول يسعى لتحسين نظام الرد على الهجمات الإلكترونية وسرعة التعامل معها، بينما يسعى العنصر الثاني والثالث والرابع إلى الرد الاستباقي من خلال تقليل فرص التعرض للهجوم الإلكتروني، بينما يسعى العنصر الخامس إلى تعظيم التعاون الدولي في مجال مكافحة الهجمات الإلكترونية.

وقد وضعت الاستراتيجية بعض المسؤوليات على الحكومة الفيدرالية، خاصة على وزارة الأمن الداخلي التي تم استحداثها بقرار رئاسي عام 2002، ومن هذه الاختصاصات:

1- تطوير خطة قومية شاملة لتأمين البنية التحتية الحرجة للولايات المتحدة ومصادرها.

2- تقديم نموذج لإدارة الأزمات للرد على أي محاولات هجوم على أنظمة المعلومات.

3- توفير المعونة الفنية للقطاع الخاص والجهات الحكومية في حالة أي هجوم إلكتروني.

4- التنسيق بين مختلف المؤسسات والوكالات الرسمية وغير الرسمية وتقديم النصائح والمعلومات بشأن الإجراءات التي يجب اتخاذها لتدعيم الأمن الإلكتروني.

ج- الاستراتيجية القومية العسكرية لعمليات الفضاء الإلكتروني

The National Military Strategy For Cyberspace Operations.

وقد صدرت هذه الاستراتيجية في 2006 وهي عبارة عن استراتيجية للقوات المسلحة الأمريكية تسعى لتحقيق هدف رئيسي هو: **تحقيق التفوق وبسط نفوذ القوات المسلحة الأمريكية على الفضاء الإلكتروني**، وتعتبر بمنزلة إطار استراتيجي عسكري ومرجع أساسي لعمل وزارة الدفاع والهيئات الدفاعية المعنية بالمجالات العسكرية، والاستخبارات، والعمليات التجارية في وعبر الفضاء الإلكتروني[1].

تسعى لتحقيق هذا الهدف من خلال[2]:

1- عمليات المعلومات وعمليات الشبكات Information Operations, Network Operations والتي تساعد في السيطرة على المعلومات وسرعة تبادلها وتوظيفها بما يخدم الأهداف المنشودة من دون التلاعب فيها أو تدميرها والقدرة على اختراق ومراقبة بيانات العدو باستمرار.

2- التطبيقات الحركية Kinetic Actions والتي تضمن حرية الحركة داخل الفضاء الإلكتروني، سواء من خلال حركات هجومية أو دفاعية أو كلاهما معاً لتحقيق الأهداف العسكرية المنشودة.

3- تطبيق القانون Law Enforcement حيث أكدت الاستراتيجية على سرعة إجراء التحقيقات في الأعمال الإجرامية وتطبيق القانون بما يمثل عملية ردع للجناة عن تحقيق أهدافهم.

4- مكافحة التجسس Counter intelligence من خلال معرفة الخصم وتحديد نواياه وأهدافه وقدراته واستغلال العمليات الإلكترونية التي يقوم بها الخصم لتحقيق الأهداف المرجوة.

1-**The National Military Strategy For Cyberspace Operations**, (The White House, December 2006) p 1.
2- Ibid, p 14-15.

5- بث موضوعات ورسائل Themes and Messages إلى الجمهور المستهدف عبر الإنترنت لخلق تعاطف مع سياسات وأهداف محددة.

تحدد هذه الاستراتيجية أربع أولويات هي[1]:

- استمرار المبادرات التي تسعى للتأثير على قرارات العدو عبر الفضاء الإلكتروني.
- توظيف قدرات الفضاء الإلكتروني في تنفيذ العمليات العسكرية.
- بناء وتعزيز القدرات من أجل تطوير عمليات الفضاء الإلكتروني
- إدارة المخاطر لعمليات الفضاء الإلكتروني.

د- المبادرة الوطنية الشاملة للأمن الإلكتروني

Comprehensive National Cybersecurity Initiative, CNCI.

قامت إدارة الرئيس بوش في يناير 2008 بإطلاق مبادرة للأمن الإلكتروني الأمريكي تؤسس نهجاً متعدد الجوانب للحكومة الاتحادية تسعى من خلاله لتحديد وتقليل التهديدات الإلكترونية الحالية والمستقبلية، والحد من نقاط الضعف التي تواجه قطاع الاتصالات والأمن الإلكتروني، والرد الفوري أو الاستباقي على الكيانات التي تسعى لسرقة أو إساءة التصرف بالمعلومات والأنظمة الإلكترونية المؤمنة[2].

1- Ibid, p x.

2-John Rollins, and Anna Chenning, **Comprehensive national cyber security initiative: legal authorities and policy recommendations national cyberstrategy,(** Congressional research service, 10 march 2009), p summary .

وتسعى هذه المبادرة لتحقيق ثلاث أهداف رئيسية هي[1]:

1- إنشاء خطوط أمامية للدفاع ضد التهديدات اليومية والفورية، وذلك من خلال زيادة التوعية بمخاطر الفضاء الإلكتروني ومواطن الضعف والتهديدات التي يحتملها وذلك بتعاون الحكومة مع مختلف الجهات الحكومية وغير الحكومية حتى يمكن تقليل مواطن الضعف وعمليات الاختراق بشبكة المعلومات.

2- صد جميع أنواع التهديدات الإلكترونية التي تواجه الولايات المتحدة الأمريكية من خلال تعزيز قدرات مكافحة التجسس الأمريكي وزيادة أمن تكنولوجيا المعلومات.

3- تدعيم مستقبل بيئة الأمن الإلكتروني، ويتم تحقيق ذلك من خلال نشر ثقافة التعليم الإلكتروني، وإعادة توجيه الجهود البحثية والتنسيق بينها وتطويرها من خلال الحكومة الفيدرالية، وتطوير استراتيجيات للتعامل مع المخاطر الإلكترونية.

ويمكن تحقيق هذه الأهداف من خلال الآليات التالية التي حددتها المبادرة:

1- التحرك نحو إدارة شبكة فيدرالية واحدة.

2- نشر أنظمة التحري والكشف عن الهوية.

3- تطوير ونشر أدوات منع الاختراق.

4- إعادة توجيه مجالات البحوث وإعادة النظر في تمويلها.

5- الربط الشبكي لمراكز العمليات الإلكترونية للحكومة الاتحادية.

1- **The Comprehensive National Cybersecurity Initiative**, On http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiativeOnOct 22th, 2013.

6- تطوير خطة حكومية قائمة على مخابرات إلكترونية واسعة.

7- زيادة أمن الشبكات السرية.

8- توسيع نطاق التعليم الإلكتروني.

9- تحديد التكنولوجيات المستقبلية التي تجعل الولايات المتحدة متقدمة عن غيرها.

10- تحديد الأدوات التكنولوجيا والبرامجية التي تدعم عملية الردع الإلكتروني.

11- وضع مناهج متعدد الجوانب لزيادة كفاءة عملية إدارة المخاطر.

12- تحديد دور الأمن الإلكتروني في مجالات القطاع الخاص.

وفي السياق نفسه حددت المبادرة أربع وكالات حكومية تتولى مسؤوليات تنفيذها تتمثل فيما يلي:

- **وزارة الأمن الوطني Homeland Security Department:** وتتولى حماية الأنظمة المعلوماتية الخاصة بالوكالات المدنية الأميركية، بما في ذلك تحصين نقاط الولوج الخارجية ونشر مستشعرات على الشبكات، فضلاً عن عقد اتفاقات شراكة وتعاون مع شركات خاصة.

- **وزارة الدفاع وتقوم بمراقبة الأنظمة المعلوماتية العسكرية:**مع تعزيز أمن الشبكات التي تتعاطى البيانات السرية ونشر نظم وقائية للحؤول دون تسريب البيانات.

- **مكتب مدير المخابرات الوطنية Office Of The Director Of National Intelligence, DNI:**الذي يتولى مراقبة أنظمة المعلومات الخاصة بالوكالات المخابراتية الأميركية ونشاطاتها، بما في ذلك وضع خطة حكومية شاملة لمجابهة الإجرام المعلوماتي.

- وأخيراً وليس آخراً **مكتب سياسة العلوم والتكنولوجيا Office Of Science And Technology Policy** التابع للرئاسة الأميركية، والمسؤول عن عدد من مشاريع الأبحاث والتطوير التي تم وضعها في إطار مبادرة CNCI.

كما أن بعض الوزارات والوكالات الاتحادية الأميركية الأخرى، مثل مكتب الميزانية التابع للرئاسة ووزارة العدل ومجلس الأمن القوميNational Security Council وغيرها تضطلع بأدوار توجيهية في عدد من مشاريع المبادرة، ويقوم سلاح الجو الأميركي بإجراء "مناورات" معلوماتية لتشبيه شن هجمات إلكترونية على الولايات المتحدة مع مشاركة عدد من الطلاب في هذه المناورات التي تُسهل وضع استراتيجيات فعالة للتصدي للهجمات المعلوماتية"[1].

1- الجيل الجديد من المحاربين الكمبيوتريين في الولايات المتحدة وإسرائيل، **مجلة الكمبيوتر والاتصالات والإلكترونيات**، النسخة الدولية، العدد 9، المجلد 30، نوفمبر 2013، يمكن المطالعة على .
http://www.accemagazine.com/article.php?categoryID=1&articleID=157

وفيما يتعلق بأبرز البرامج والأدوات الأمريكية في مجال توظيف القوة الإلكترونية في عهد إدارة بوش الابن فنجد أن:

بعد هجمات الحادي عشر من سبتمبر عملت وكالة الأمن القومي الأمريكي على إنشاء العديد من البرامج بهدف مكافحة العمليات الإرهابية، وقد ساهمت التسريبات التي قام بها سنودن في كشف العديد من البرامج والأدوات التي استخدمتها الولايات المتحدة في ممارسة قوتها الإلكترونية، وعلى الرغم مما كشفت عنه هذه التسريبات، فإن الكاتب يرى أن هناك كثيراً من البرامج الأخرى لدى الولايات المتحدة التي مازالت تعمل سراً، وما سوف نتطرق إليه هو ما كشفت عنه التسريبات، والتي تعكس قدرة الولايات المتحدة على التجسس وجمع البيانات عبر الإنترنت، سواء كانت لأهداف داخل الولايات المتحدة أو خارجها، ولعل أبرزها هو برنامج بريسم Prism، حيث تهدف وكالة الأمن القومي الأمريكي من هذه البرامج إلى مراقبة أنشطة الأفراد المشتبه بهم، بل وغير المشتبه أيضاً، من خلال تتبع مكالماتهم الهاتفية ومراسلاتهم الإلكترونية.

وفي هذا الصدد تجمع وكالة الأمن القومي نوعين من المعلومات[1]:

-Metadata أو البيانات العملاقة: والتي تشمل تسجيل المكالمات الهاتفية، والموقع الجغرافي Geolocation Data للهدف من خلال IP Addresses المستخدم في عمليات التواصل الإلكتروني وسجلات البحث على الإنترنت Web Search Histories.

-Content أو المحتوى: والذي يشمل المراسلات الإلكترونية والمحادثات الفورية عبر الإنترنت، والملفات المخزنة على خوادم وأجهزة حسابات شخصية.

1-**Everything you need to know about PRISM**, Access Date, August 25th, 2014, on http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet

ومن أبرز البرامج التي كشفت عنها التسريبات في عهد إدارة بوش هو:

:Wind Stellar

أحد برامج التجسس الإلكترونية الرئيسية التي ظهرت بعد أحداث الحادي عشر من سبتمبرمباشرة، وكان الغرض منه هو التجسس المحلي على المقيمين داخل الأراضي الأمريكية، ويعمل البرنامج على التجسس على الاتصالات الهاتفية والمراسلات الإلكترونية[1]،وقد استمر هذا البرنامج لمدة عامين في ظل إدارة الرئيس أوباما الأولى قبل أن ينهى عمله ويتم استبداله ببرامج أخرى مثل "Evilolive" And "Shelltrumpet."

:PRISM

بموجب قانون حماية أمريكا الصادر في عام[2]Protect America Act of 2007 تم إنشاء برنامج سري يدعى US-984XN ويدعى أيضاً PRISM، وهو أحد البرامج التي تم تصميمها في إطار مكافحة الإرهاب، ويعمل برنامج "بريسم" على جمع معلومات من أشخاص، سواء داخل أو خارج الولايات المتحدة، وبموجب قانون حماية أمريكا، وبمجرد موافقة أحد القضاة السريين بمحكمة مراقبة الاستخبارات الخارجية التي تم إنشاؤها بموجب القانون، يحق لوكالة الأمن القومي الأمريكي NSA أن تطلب من الشركات العاملة في مجال الإنترنت، مثل ياهو وفيس بوك وجول وأبل ومايكروسوفت غيرها، بيانات تتعلق بمستخدمين لها حول العالم[3].

1- Justice Department and NSA memos proposing broader powers for NSA to collect data**, The Guardian,**Access Date, August 26th, 2014, on
http://www.theguardian.com/world/interactive/2013/jun/27/nsa-data-collection-justice-department.

2- هو تطوير لقانون مراقبة الاستخبارات الخارجية Foreign Intelligence Surveillance Act، بهدف تمكين الولايات المتحدة من مراقبة أنشطة الجماعات الإرهابية بعد أحداث 11 سبتمبر، يمكن مطالعة نص القانون على الرابط التالي:
http://www.justice.gov/archive/ll/

3-Secret program gives NSA, FBI backdoor access to Apple, Google, Facebook, Microsoft data ,**the Verge,** Access Date, August 25th, 2014, on.
http://www.theverge.com/2013/6/6/4403868/nsa-fbi-mine-data-apple-google-facebook-microsoft-others-prism/in/4167369

قام إدوارد سنودنEdward Snowden الموظف السابق بوكالة الاستخبارات الأمريكية CIA وبوكالة الأمن القومي الأمريكية NAS بتسريب معلومات لصحيفة الجارديان البريطانية حول برنامج بريسمفي يونيو 2013، وهو برنامج تجسس رقمي أمريكي مصنف بأنه سري للغاية يُشّغل من قبل وكالة الأمن القومي الأمريكية (NSA) بدأ منذ عام 2007، حيث يتيح مراقبة الاتصالات الحية والمعلومات المخزنة، واستهداف أي عميل لأي شركة منخرطة في البرنامج، مثل شركة جوجل وفيسبوك وتويتر وغيرها، في حال كان هذا العميل يسكن خارج الولايات المتحدة، أو كان مواطناً أمريكياً له اتصالات تتضمن محتويات خاصة بأشخاص خارج الولايات المتحدة، حيث يستطيع هذا البرنامج الحصول على معلومات تتضمن، رسائل البريد الإلكتروني، ومحادثات الفيديو والصوت، والصور، والاتصالات الصوتية ببرتوكول الإنترنت، وعمليات نقل الملفات، وإخطارات الولوج وتفاصيل الشبكات الاجتماعية[1].

1- NSA Prism program slides, **The Guardian,** On Nov 5th, 2013, http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document

ثانياً: القوة الإلكترونية في إطار إدارة الرئيس أوباما (2008-2012):

تعرض الرئيس أوباما لخطر التهديدات الإلكترونية مبكراً، حيث تعرضت حملته الانتخابية لاختراق إلكتروني من قراصنة صينيين استهدفوا مسودات الوثائق الخاصة بالسياسات التي سوف يتبعها حال فوزه رئيساً للولايات المتحدة الأمريكية[1]، أولت إدارة الرئيس الأمريكي باراك أوباما اهتماماً كبيراً بمجال الأمن الإلكتروني، حيث أكد الرئيس الأمريكي في خطاب له أثناء حملته الرئاسية أن التهديدات الإلكترونية من أخطر التحديات التي تواجه الاقتصاد والأمن القومي الأمريكي، وأن رفاهية الاقتصاد الأمريكي في القرن الحادي والعشرين سوف تعتمد على الأمن الإلكتروني[2].

وبمجرد توليه مهام الرئاسة كلف الرئيس أوباما فريق عمل من مختلف الجهات والرسمية وغير الرسمية بإعادة تقييم الخطط والاستراتيجيات الخاصة بالأمن الإلكتروني الأمريكي، وقد أنهي هذا الفريق عمله بإصدار تقرير بعنوان "مراجعة سياسة الفضاء الإلكتروني Cyberspace Policy Review".

1- ريتشارد كلاركو روبرتنيك، **حر بالفضاء الإلكتروني** .. التهديد التالي للأمن القومي وكيفية التعامل معه، مركز الإمارات للدراسات والبحوث الاستراتيجية، 2012، صص 145- 146.

2- President Obama, Speech at Purdue University, July 17th, 2008.

وكان أبرز ما جاء بالتقرير المحاور التالية[1]:

1- أهمية البيئة الإلكترونية للأمة الأمريكية:

تتمثل أهم بنود هذا المحور فيما يلي:

أ- البنية الرقمية للاتصالات والمعلومات والمرتبطة عالمياً مع بعضها البعض والتي تعرف بأنها الفضاء الإلكتروني، تدعم تقريباً كل جوانب المجتمع الأمريكي، حيث توفر دعماً حيوياً للاقتصاد الأمريكي، والبنية التحتية المدنية، والسلامة العامة للمواطنين، والأمن القومي الأمريكي.

ب- تعتبر التهديدات الإلكترونية من أخطر التحديات التي تواجه الأمة الأمريكية والاقتصاد الأمريكي في القرن الحادي والعشرين.

ج- تم تجهيز البنية التحتية الرقمية بحيث تكون سهلة وقابلة بسهولة للتشغيل، وقد جاء ذلك على حساب التعزيزات الأمنية، مما جعل بعض الفواعل - سواء من الدول أو غيرها - تعبث بها وتسعى لسرقة أو تضليل أو تدمير المعلومات الرقمية، وهو ما قد يسبب تدمير للأنظمة الإلكترونية الأمريكية.

د- تسعى الولايات المتحدة إلى مواجهة معضلة مزدوجة وهي إيجاد بيئة إلكترونية تدعم الإبداع والكفاءة والرخاء الاقتصادي وحرية التجارة، وفي نفس الوقت تكون آمنة ومؤمنة وتدعم الحريات المدنية وحقوق الملكية.

هـ- إنها لمسؤولية رئيسية على حكومة الولايات المتحدة أن تواجه التحديات الاستراتيجية في الفضاء الإلكتروني وتعمل على تعظيم استفادتها واستفادة العالم كله من إمكانيات الثورة المعلوماتية.

1- **Cyberspace Policy Review**, (The Office of the White House, May 29, 2009), p iii – vii.

2- أهمية الحوار الوطني لمواجهة التهديدات الإلكترونية:

أ- يجب على الولايات المتحدة أن ترسل رسالة قوية إلى العالم تؤكد فيها سعيها لمواجهة التهديدات الإلكترونية بقيادة ورؤية جادة، هذه القيادة يجب أن ترتكز داخل البيت الأبيض من أجل توفير التوجيه والتنسيق لتحقيق النتائج المرجوة، كما يجب تدعيم القيادة الفيدرالية المسؤولة عن الأمن الإلكتروني.

ب- هذا المنهج الجديد يتطلب تحديد الأدوار والمسؤوليات للوكالات والهيئات الفيدرالية، بالإضافة إلى توفير الخطط والاستراتيجيات والغطاء القانوني اللازم لإتمام هذه المهمة.

ج- يجب على الحكومة الأمريكية أن تقوم بالتعاون مع قطاع الصناعات بشرح التحديات الإلكترونية الحالية، وطرح الحلول اللازمة للتغلب عليها، مما يجعل المواطنين الأمريكيين يشعرون بأهمية الحاجة إلى قيام الحكومة باتخاذ الإجراءات اللازمة.

د- يجب أن تقوم الحكومة الفيدرالية بعمل حملات توعية وتعليم ناجحة حول مخاطر الفضاء الإلكتروني، فالمواطنون لن يقدروا أهمية الأمن الإلكتروني قبل أن يعرفوا أولاً المخاطر التي قد يتعرضون لها.

هـ- يجب على حكومة الولايات المتحدة أن تعمل في شراكة مع القطاع الخاص، حيث يشارك القطاع الخاص القطاع العام في مسؤولية إيجاد بنية تحتية مؤمنة وموثوق بها.

و- هذه الشراكة بين القطاع الخاص والقطاع العام يجب أن تكون مُعرّفة بحيث يتم تحديد أدوار كل منهما بصورة واضحة ومحددة، وتعطي أولوية لاتخاذ القرارات المنشودة بصورة فعالة لتأمين الفضاء الإلكتروني.

ز- الأمة الأمريكية في حاجة إلى وجود استراتيجية للأمن الإلكتروني يمكن من خلالها إعادة تشكيل البيئة الدولية، بحيث تشارك الدول التي تتلاقى معها في مبادئ ومعايير معينة، وهو ما يساهم في إنشاء بنية تحتية رقمية مؤمنة ومشتركة بينهم.

ح- **قضايا مثل مكافحة الجريمة الإلكترونية،** والحفاظ على البيانات، وتدعيم الشبكات الإلكترونية، والحفاظ على الخصوصية، والقدرة على صد الهجمات الإلكترونية، كلها تحديات يجب التصدي لها لخلق حكومة إلكترونية مؤمنة، ولن تتمكن الولايات المتحدة من مواجهة هذه التحديات إلا من خلال العمل المشترك مع الشركاء الدوليين.

ط- **تعمل الولايات المتحدة مع الشركاء المحليين والدوليين والقطاع الخاص** للتنسيق من أجل حماية البنية التحتية والمعلومات والاتصالات، ويجب أن تعمل على تحفيز السوق وقطاع الأعمال لجعل المنتجات والخدمات العامة أكثر أمناً، وذلك من خلال برامج التحفيز كالضرائب وغيرها.

ى- **يجب على الولايات المتحدة أن تعمل على تعظيم الاستفادة من التكنولوجيا** الحديثة لسد احتياجات الاقتصاد والأمن الوطني.

3- مسؤولية الحكومة الفيدرالية عن حماية الدولة من الهجمات الإلكترونية:

ينص هذا المحور على أن الحكومة الفيدرالية مسؤولة بصورة كاملة عن الحفاظ وتدعيم أمن المواطنين، **ومن ثم:**

أ- إن الولايات المتحدة في حاجة إلى إطار شامل لتنسيق الجهود بين الحكومات المحلية والفيدرالية والسلطات المحلية والقطاع الخاص والمجتمع الدولي للرد على الهجمات المحتملة.

ب- يجب على الحكومة والمستفيدين المتعاملين معها تطوير آلية تعمل على دمج البيانات بين الحكومة والقطاع الخاص لمعرفة نقاط الضعف وتقويتها ووضع احتمالات للرد على محاولات اختراقها.

ج- المنهج المتبع في الأمن الإلكتروني خلال الـ 15 عاماً الماضية لم ينجح في منع التهديدات الإلكترونية، ومن ثم فهناك حاجة إلى كيان يأخذ مسؤولية الحفاظ على الأمن الإلكتروني الأمريكي بجدية، وهذا يتطلب أن يتولى البيت الأبيض هذه المسؤولية.

وانعكاساً لما سبق، احتل هدف تعزيز أمن الفضاء الإلكتروني أولويات اهتمام إدارة الرئيس الأمريكي أوباما، ويمكن تتبع ذلك على النحو التالي:

- إنشاء قيادة عسكرية في الفضاء الإلكتروني تابعة للبنتاجون:

فقد أكدت "استراتيجية الاستخبارات القومية للولايات المتحدة" لعام 2009 على ضرورة مكافحة "التطرف العنيف"، وتخلت عن هدف تعزيز الديمقراطية ومساعدة الدول الديمقراطية ضمن أهداف الاستخبارات التي وردت باستراتيجية الاستخبارات القومية لعام 2005، وطرحت بدلاً منها هدف تعزيز أمن الفضاء الإلكتروني[1].

لذلك استحدث البنتاجون في يونيو 2009 قيادة عسكرية مهمتها الرد على هجمات قراصنة المعلوماتية وتنفيذ عمليات في الفضاء الإلكتروني. فالأخطار المرتبطة بأمن الفضاء الإلكتروني هي من أخطر التحديات التي يواجهها الاقتصاد والأمن القومي في القرن الحادي والعشرين[2]. وقد تم تعيين أول جنرال عسكري لإدارة حروب الفضاء الإلكتروني هو الجنرال إلكسندر كيث، وجاء قرار البنتاجون بإنشاء تلك القيادة ليمثل طوراً جديداً في مجال الحرب الإلكترونية عن طريق الفضاء الالكتروني، وتستهدف وزارة الدفاع الأمريكية من تلك القيادة الجديدة أن تشرف على مختلف الجهود المتعلقة بالإنترنت في كل أجهزة القوات المسلحة، مع التأكيد أنها لن تصل إلى مستوى عسكرة فضاء الإنترنت.

ومنذ خطاب الرئيس الذي شكّل مَعْلَماً بارزاً حول أمن الفضاء الإلكتروني في مايو 2009، عينت الحكومة هوارد شميت منسقاً لأمن الفضاء الإلكتروني في هيئة موظفي الأمن القومي. وقد أطلق السيد شميت وفريق عمله المبادرة القومية لتعليم أمن الفضاء الإلكتروني (NICE)[3].

1- معتز سلامة، "استراتيجية الأمن القومي الأمريكي 2010"، **كراسات استراتيجية،** 1 أبريل 2010، يمكن المطالعة على
http://digital.ahram.org.eg/articles.aspx?Serial=657085&eid=2920

2- عادل عبد الصادق، أمريكا وتشكيل قيادة عسكرية في الفضاء الالكتروني ..هل بدأ الاستعداد لحروب المستقبل؟، **مجلة تعليقات مصرية،** عدد 130، (مركز الأهرام للدراسات السياسية والاستراتيجية، يوليو 2009)، يمكن المطالعة على
http://acpss.ahram.org.eg/Ahram/2009/7/12/COMM0.HTM

3- تلخيص استراتيجية التجدد القومي، القيادة العالمية للقرن الحادي والعشرين، **موقع السفارة الأمريكية،** تاريخ دخول 2 مايو 2012.
http://iipdigital.usembassy.gov/st/arabic/article/2010/06/20100602110620snmassabla7.860965e-02.html#axzz2h2UwS1hZ

وفي مقال نشره "كيث" أوضح فيه استراتيجية عمل هذه القيادة الجديدة، والتي تتركز في[1]:

- اعتبار الفضاء الإلكتروني نطاقاً واحداً يخدم أهدافاً تنظيمية وتدريبية وتجهيزية، بما يسمح لوزارة الدفاع أن تستفيد إلى أقصى حد ممكن من إمكانياتها العسكرية الاستخباراتية وإمكانياتها في الأعمال التجارية.

- استخدام مفاهيم جديدة للعمل الدفاعي، بما فيها دفاعات إلكترونية ناشطة، مثل مراقبة الحركات الإلكترونية من أجل حماية شبكات وزارة الدفاع وأنظمتها.

- العمل بالاشتراك مع وزارات وأنظمة أمريكية أخرى ومع القطاع الخاص من أجل تنشيط استراتيجية تشمل كامل الحكومة ومن أجل اتباع مقاربة وطنية شاملة لأمن الفضاء الإلكتروني.

- الاستفادة من مؤهلات المواطنين ذوي الخبرات العالية، وذلك عن طريق توظيف قوى عاملة إلكترونية ماهرة والحفاظ عليها وعبر تمكين الابتكار التقني السريع.

وتتركز المهمة الرئيسية لهذه القيادة على حماية شبكات وزارة الدفاع وأنظمتها، والاستعداد لخوض الحروب والدفاع عن شبكات الدولة الأمريكية، من خلال إدارة عمليات شبكات المعلومات التابعة لوزارة الدفاع الأمريكي، لتحقيق هدفين رئيسيين هما، حماية حرية عمل الولايات المتحدة وحرية عمل حلفائها في الفضاء الإلكتروني، وحرمان أعداء الولايات المتحدة –عند الطلب– من حرية العمل في الفضاء الإلكتروني.

1- Gen Keith B. Alexander, **Building A New Command in Cyberspace**, Strategic Studies Quarterly, , USA, Summer 2011, pp. 3–12. On http://www.au.af.mil/au/ssq/2011/summer/alexander.pdf

استراتيجية الأمن القومي الأمريكي 2010:

حظى الفضاء الإلكتروني باهتمام استراتيجية الأمن القومي للرئيس أوباما للعام 2010، حيث اعتبرت أن "الخطر الأكبر على الشعب الأمريكي والأمن العالمي لا يزال يأتي من: أسلحة الدمار الشامل، خاصة النووية، ومن الفضاء، وقدرات الفضاء الإلكتروني التي تجعل حياتنا اليومية والعمليات العسكرية عرضة للاضطراب والهجوم، والاعتماد على الوقود الحيوي الذي يقيد خياراتنا ويلوث بيئتنا، والتغير المناخي والأمراض الوبائية التي تهدد أمن الأقاليم وصحة وسلامة الشعب الأمريكي، والدول الفاشلة التي تولد الصراع وتهدد الأمن الإقليمي والعالمي، والشبكات الإجرامية العالمية التي تغذي انعدام الأمن في الخارج، وتأتي بالناس والبضائع عبر حدودنا ليهددوا شعبنا"[1]. ومن ثم يجب تدعيمهما لمواجهة أي تهديدات غير تقليدية.

وقد حددت استراتيجية الأمن القومي للعام 2010 عدة تهديدات رئيسية هي: الإرهاب، الكوارث الطبيعية، الهجمات الإلكترونية على نطاق واسع، والأوبئة، وأكدت على أهمية مواجهة هذه التهديدات على مختلف المستويات، سواء في البر أو البحر أو الجو أو الفضاء الكوني أو الفضاء الإلكتروني[2].

وتنظر الاستراتيجية إلى أن التهديدات الإلكترونية تمثل أحد أخطر التهديدات التي تواجه الأمن القومي والسلامة العامة للمواطنين، فضلاً عن أنها أحد أهم التحديات التي تواجه الاقتصاد القومي، ومن ثم يجب تأمينها وأن تكون جديرة بثقة مستخدميها، ويمكن تحقيق ذلك عبر الاستثمار في الناس والتكنولوجيا، وعبر تدعيم الشركات مع القطاعات المختلفةسواء أفراداً أو مؤسسات خاصة[3].

1- **National Security Strategy 2010**, (The White House, May 2010), pp. 8-10.
2- Ibid pp. 8-10.
3- Ibid.,pp. 27-28.

الاستراتيجية الدولية للفضاء الإلكتروني:

كشفت وزيرة الخارجية الاميركية هيلاري كلينتون في مايو 2011 عن استراتيجية دولية للفضاء الإلكتروني بهدف تشجيع بنية تحتية مفتوحة وآمنة للمعلومات والاتصالات. وتأتي هذه الاستراتيجية في أعقاب الثورات الشعبية التي اجتاحت منطقة الشرق الأوسط وأشعلتها مواقع الإنترنت، خاصة مواقع التواصل الاجتماعي، حيث أوضحت كلينتون في مؤتمر صحفي للكشف عن الاستراتيجية أن الولايات المتحدة ستعمل على مستوى دولي لتشجيع بنية تحتية مفتوحة وقابلة للتشغيل المتبادل وآمنة موثوق بها تدعم التبادل التجاري وتعزز الأمن الدولي وتعزز حرية الرأي والابتكار[1].

حيث تحدد الاستراتيجية عدة أولويات تسعى لتحقيقها، وتعتبرها بمنزلة حتمية جديدة للسياسة الخارجية الأمريكية، هذه الأولويات هي[2]:

- المشاركة الاقتصادية لتشجيع الابتكار والتجارة مع حماية الملكية الفكرية في الوقت نفسه.

- أمن الفضاء الإلكتروني من أجل حماية الشبكات الإلكترونية وتعزيز الأمن الدولي.

- تطبيق القانون لتحسين قدرة الولايات المتحدة على الرد على جرائم الفضاء الإلكتروني وذلك من خلال تعزيز القوانين الدولية، حيث يكون ذلك مناسباً.

- التعاون العسكري لمساعدة حلفاء الولايات المتحدة في المزيد من العمل معاً في مواجهة أخطار الفضاء الإلكتروني مع ضمان بقاء شبكاتنا العسكرية محمية.

1- نص كلمة وزيرة الخارجية الأمريكية، **موقع السفارة الأمريكية**، بتاريخ دخول 4 يونيه 2012،على الرابط التالي:
http://iipdigital.usembassy.gov/st/arabic/texttrans/2011/05/20110517155359x0.5792004.html#ixzz2jDH4pFE6

2-**International Strategy For Cyberspace**, (The White House, May 2011) pp 17-23.

- الحكم الرشيد لأصحاب المصالح المتعددة في الإنترنت، بحيث تعمل الشبكات كما يجب.

- التنمية لدعم نهوض شركاء جدد من خلال مساعدة البلدان في تطوير بنيتها الرقمية الأساسية وبناء إمكانياتها بحيث تواجه وتتحمل أخطار الفضاء الإلكتروني.

- ضمان حرية الإنترنت والعمل المشترك لزيادة حماية الخصوصية وضمان الحريات الأساسية للتعبير والتجمع وتنظيم الجمعيات على الإنترنت.

فيما يتعلق بالبرامج والأدوات التي استخدمتها إدارة الرئيس أوباما فنجد أنه:

استمر عمل برنامج بريسم، في حين توقفت برامج أخرى وتم استبدالها ببرامج أقوى تحقق السيطرة الأمريكية على الفضاء الإلكتروني، ومنها:

- برنامج السيطرة على الأجهزة من خلال ترددات الراديو:

تمثل الأجهزة غير المتصلة بالإنترنت أو بأي شبكة داخلية مشكلة حقيقة في إمكانية التجسس عليها أو اختراقها، على عكس الأجهزة المتصلة بشبكة الإنترنت، وهو ما دفع وكالة الاستخبارات الأمريكية في عام 2008 لتطوير برنامج جديد يستخدم موجات الراديو لاختراق الحاسبات غير المتصلة بالإنترنت، وذلك عبر إدراج برنامج صغير على جهاز الكمبيوتر من خلال ذاكرة صلبة، يعمل كمستقبل ومرسل للبيانات في نفس الوقت Transceiver، على مدى يصل إلى 7 أميال، في هذا المدى يوجد جهاز كمبيوتر محمول مخصص يعمل على استقبال هذه الموجات وإرسالها إلى المحطة المركزية من أي مكان في العالم، ومن ثم فأصبح بالإمكان التغلب على مشكلة اختراق الأجهزة غير المتصلة بالإنترنت، ولكن يظل العامل البشري مهماً في إدخال برنامج التجسس على جهاز الكمبيوتر بصورة يدوية[1].

- برنامج المواطن المثالي Perfect Citizen:

ويقوم هذا البرنامج على وضع أجهزة استشعار في شبكات تشغل البنية التحتية الحساسة، مثل شبكة الكهرباء ومحطات الطاقة النووية، تعمل هذه الأجهزة على

1-**N.S.A. Devises Radio Pathway Into Computers,** New Yorktimes, On Jan 14th, 2014 http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html?_r=1&utm_source=Sailthru&utm_medium=email&utm_term=%2AMorning%20Brief&utm_campaign=MB%201.15.14

إرسال إنذارات بمجرد الاشتباه في أي هجمات إلكترونية ضد البنية التحتية، حيث يوفر هذا البرنامج مجموعة من الحلول التقنية التي تساعد وكالة الأمن القومي على فهم التهديدات التي تتعرض لها شبكات الأمن القومي بشكل أفضل[1].

وقد بدأت خطوات تنفيذ البرنامج في يوليو 2010 في سرية تامة بمنح حق تنفيذ المشروع لإحدى الشركات، إلى أن كشفت صحيفة وول ستريت جورنال عن هذا المشروع.

وقد أثار البرنامج القلق حول مصير الخصوصية في الإنترنت، وعما إذا كان هدف البرنامج هو التجسس على المواطنين أم لا، وهو الأمر الذي تم نفيه من قبل المسؤولين، حيث أكدت "جوديثإيميل" وهي متحدثة باسم وكالة الأمن القومي أن هذا البرنامج ليس لديه قدرة على تعقب أو مراقبة الاتصالات عبر شبكة الإنترنت، وهو مجرد أجهزة حساسة لوقف الهجمات الإلكترونية على المرافق الحيوية، وأضافت أن البرنامج هو عبارة عن "جهد بحثي وهندسي، ولا ينطوي على نشاط مراقبة"[2].

EvilOlive

هو البرنامج الرئيسي الذي حل محل برنامج Stellar wind، وذلك في عام 2011، وكان الهدف الرئيسي منه هو جمع كميات كبيرة من المعلومات العملاقة الموجودة على الإنترنت، سواء كانت اتصالات أو معلومات، تخص أفراداً داخل أو خارج الولايات المتحدة، حيث يستطيع هذا البرنامج أن يجمع نصف البيانات الحية التي يتم تراسلها عبر الإنترنت، وهو ما يعتبر نقلة نوعية في القدرات الكمية لبرامج التجسس، من حيث القدرة على جمع أكبر قدر من المعلومات[3].

1- U.S. Plans Cyber Shield for Utilities, Companies, **The wall street Journal**, http://online.wsj.com/news/articles/SB10001424052748704545004575352983850463108 on October 20th, 2013.
2- **NSA offers explanation of Perfect Citizen**, http://news.cnet.com/8301-1009_3-20010155-83.htmlon October 20th, 2013.
3- Glenn Greenwald and Spencer Ackerman, How the NSA is still harvesting your online data**, The Guardian,** June 17, 2014,Accessed August 26th, 2014 On: http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection

ShellTrumpet

وقد تم الإعلان عن هذا البرنامج عام 2012، ويعمل على جمع بيانات عملاقة عبر الإنترنت من مختلف المستخدمين، ويفوق هذا البرنامج في قدراته برنامج EvilOlive، حيث تم الإعلان في ديسمبر 2012 أن هذا البرنامج مع تريليونات من البيانات العملاقة، نصفها فقط تم في عام 2012[1].

اختراق الأجهزة الشخصية عبر التطبيقات الاجتماعية:

لما كان الاعتماد على الأجهزة المحمولة يتزايد، مثل الهاتف المحمول والحاسب اللوحي وغيرها، فقد أصبحت هدفاً للإدارة الأمريكية، لما يمكن أن توفره من معلومات حول مستخدميها، خاصة إذا كان هذا المستخدم هدفاً لأحد الأجهزة الأمريكية، فيمكن اختراق بعض تطبيقات الهاتف المحمول ومعرفة مكان هذا الشخص، وسرقة المعلومات الموجودة على هاتفه، وكذلك تستفيد الإدارة الأمريكية أيضاً من تطبيقات مواقع التواصل الاجتماعي للحصول على كافة البيانات المُخزنة في حسابات المُستخدمين، مثل العمر والجنس والميول ومكان الوجود والمُستوى العلمي وغيرها.

ومن أبرز التطبيقات التي اعتمدت عليها الولايات المتحدة لاختراق الهاتف المحمول هو تطبيق Angry Birds أو الطيور الغاضبة، وهي لعبة زائعة الصيت على الأجهزة المحمولة واللوحية، فقد كشف تقرير نشرته صحيفة "الجارديان" البريطانية، أن وكالة الأمن القومي الأميركية تقوم بتطوير تقنيات تسمح لها باستغلال تطبيقات الهواتف الذكية للوصول إلى معلومات خاصة بالمُستخدمين[2].

1-Pierluigi Paganini, Stellar Wind, Prism,EvilOlive,ShellTrumpet, US massive surveillance**, Security Affairs,** on June 29th, 2014, on http://securityaffairs.co/wordpress/15689/intelligence/stellar-wind-prism-evilolive-shelltrumpet-surveillance.html

2- Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data, **The Guardian**, Jan 28th,2014. On http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data

فقد سرب سنودن وثائق تؤكد استهداف وكالة الاستخبارات الأمريكية CIA بيانات الهاتف المحمول للمُستخدم، وذلك لجلب معلومات عن الإرهابيين وأهداف استخباراتية أُخرى، حيث أنفقت ما يزيد عن مليار دولار لصالح برامج التجسس الخاصة باستهداف الهواتف الذكية[1].

ولتوضيح قُدرة برامج الوكالة، أشار التقرير إلى أنه مجرد قيام المُستخدم برفع صورة إلى وسائل التواصل الاجتماعي باستخدام هاتفه الذكي، تستطيع الوكالة جمع معلومات مثل جهات الاتصال في هاتف المُستخدم، وعناوين البريد الإلكتروني، وموقع المُستخدم.

1- البيانات الشخصية في قبضة الـ CIA عبر "Angry bird" ، **موقع العربية**، تاريخ مطالعة 28 يناير 2014، يمكن المطالعة على:
http://www.alarabiya.net/ar/technology/2014/01/28/%D8%A7%D9%84%D8%A8%D9%8A%D8%A7%D9%86%D8%A7%D8%AA-%D8%A7%D9%84%D8%B4%D8%AE%D8%B5%D9%8A%D8%A9-%D9%81%D9%8A-%D9%82%D8%A8%D8%B6%D8%A9-%D8%A7%D9%84%D9%80-CIA%D8%B9%D8%A8%D8%B1-Angry-bird-.html

ثالثاً: كيف تعمل برامج التجسس التابعة لوكالة الأمن القومي الأمريكي:

تعمل برامج التجسس في الولايات المتحدة الأمريكية بالاستناد على قانونين رئيسيين هما: المادة 702 من القانون المعدل مراقبة الاستخبارات الخارجية The Foreign Intelligence Surveillance Act والمادة 215 من القانون الوطني Patriot Act، حيث يخول القانون الأول السلطة لوكالة الأمن القومي الأمريكي لجمع المعلومات الخاصة بالتواصل الإلكتروني من برنامج بريسم وغيره من البرامج، عبر شركات الإنترنت، ويخول الثاني السلطة لها لجمع المعلومات العملاقة الخاصة بالاتصالات الهاتفية من شركات الاتصالات[1]، وتحصل وكالة الأمن القومي على هذه البيانات إما مباشرة من خلال خطوط Upstream التي تعمل على سحب البيانات مباشرة من الكابلات البحرية التي تحمل المعلومات، أو من خلال الخوادم التي يتم تخزين هذه البيانات عليها لشركات أمريكية، مثل برنامج بريسم للحصول على المعلومات من الشركات[2].

1-Timothy B. Lee, Here's everything we know about PRISM to date, **Washington Post**, June 12, 2013, Accessed date August 28th, 2014, http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/
2- Ibid.

الخلاصة:

نخلص مما سبق إلى أن:

1- إدارة الرئيس بوش كانت تنظر إلى الفضاء الإلكتروني باعتباره أحد مصادر التهديد التي يمكن أن تستخدمه الجماعات الإرهابية كوسيط في تنفيذ عمليات عسكرية ضد الولايات المتحدة الأمريكية، ومن ثم عملت على تأمينه، خاصة البنية التحتية باعتبارها أحد الأهداف الرئيسية للعمليات الإرهابية، ومن ثم جاءت الاستراتيجيات لتؤكد على ضرورة تأمين الفضاء الإلكتروني باعتباره وسيلة لتحقيق أهداف أكبر، على الرغم من ذلك فإن هذه الاستراتيجيات لم تعط القطاع الخاص قدراً كبيراً من الاهتمام باعتباره شريك في امتلاك البنية التحتية للأنترنت، وإذا كان من شأن هذه الاستراتيجيات حفظ وتأمين البيانات الفيدرالية، فماذا عن تأمين البيانات التابعة للقطاع الخاص والشركات والمؤسسات المالية والتي من شأن تهديدها أن يؤثر على الأمن القومي الأمريكي وإن كان بصورة غير مباشرة؟ كما أن بعض المؤسسات الرسمية تعتمد على القطاع الخاص في توفير هذه الخدمات، مما يؤثر بصورة مباشرة على الأمن القومي، ولذلك فإن مستوى الأمن المعلوماتي الحكومي الأميركي لم يتحسن كثيراً نتيجة لذلك، وفق ما ورد في تقارير هيئات رقابة وتدقيق العمل الحكومي الأميركي، والأسوأ من ذلك أن فرض بعض التدابير على الدوائر الحكومية لتعزيز أمنها الكمبيوتري قد حال دون اتخاذها تدابير "بديهية" لتعزيز هذا الأمن، وفق ما جاء على لسان بعض أعضاء الكونجرس الأميركي الناظرين في هذا الشأن[1].

1- الجيل الجديد من المحاربين الكمبيوتريين في الولايات المتحدة وإسرائيل، **موقع مجلة الكمبيوتر**، بتاريخ مطالعة 28 ديسمبر 2013، يمكن المطالعة على:
http://www.accemagazine.com/article.php?categoryID=1&articleID=157

2- في المقابل نظرت إدارة الرئيس باراك أوباما إلى الفضاء الإلكتروني باعتباره أحد مصادر الرخاء والتقدم الاقتصادي للولايات المتحدة، وأكدت معظم الاستراتيجيات ضرورة بناء شراكة مع القطاع الخاص والأفراد في حد ذاتهم إلى جانب تعظيم التعاون الدولي في مجال مكافحة الهجمات الإلكترونية، وقد انعكس هذا الاهتمام في استراتيجية الدفاع القومي 2010، حيث اعتبرت الهجمات الإلكترونية بصفة عامة من أبرز التهديدات التي تواجه الولايات المتحدة الأمريكية، وهي في ذلك تختلف عن إدارة الرئيس بوش، التي اهتمت بالفضاء الإلكتروني لأنه النظام الرئيسي لإدارة البنية التحتية الأمريكية.كما أن الاستراتيجيات الأمريكية تنوعت ما بين **الهجوم** مثل الاستراتيجية القومية العسكرية لعمليات الفضاء الإلكترونية، وإنشاء قيادة عسكرية في الفضاء الإلكتروني تابعة للبنتاجون، و**الدفاع**، مثل الاستراتيجية القومية للحماية المادية للبنية التحتية الحرجة والأصول الرئيسية، والاستراتيجية القومية لتأمين الفضاء الإلكتروني وبرنامج المواطن المثالي، و**تعظيم التعاون الدولي** في مجال مكافحة الهجمات الإلكترونية، مثل الاستراتيجية الدولية للفضاء الإلكتروني، وبهذا يصبح الفضاء الإلكتروني أحد الأسلحة الرئيسية في الدفاع عن مصالح الولايات المتحدة داخلياً، أو المساعدة في تنفيذ أهدافها خارجياً، ومن ثم يمكن إضافة عنصر جديد لعناصر تنفيذ السياسة الخارجية الأمريكية، وهو القوة الإلكترونية، إلى جانب قوتها الصلبة (الاقتصادية والعسكرية)، وقوتها الناعمة (الثقافية والإعلامية).

المبحث الثالث

حدود القوة الإلكترونية الأمريكية

على الرغم من ريادة الولايات المتحدة في مجال الفضاء الإلكتروني، واعتباره مجالاً للعمليات العسكرية، وإطلاق العديد من الاستراتيجيات والوثائق التي تحكم عمل الولايات المتحدة فيه، فإن القوة الإلكترونية الأمريكية ليست مطلقة، حيث إنها مقيدة بعدة عوامل، منها مدى كفاية وجود سلطة قانونية ودستورية للرد على الهجمات الإلكترونية، والأدوار التي يمكن أن تقوم بها السلطة التنفيذية والتشريعية للرد على هذه الهجمات، والصراع المستمر بين القراصنة الإلكترونين وبرامج مكافحة التجسس الإلكتروني، فضلاً عن الاعتبارات السياسية المتمثلة في مصادرة الحريات أو التضييق على الناشطين أو اعتراض القوى الدولية على احتكار الولايات المتحدة للفضاء الإلكتروني، وانطلاقاً من ذلك يسعى هذا المبحث لتحليل أهم العوامل التي تضع حدوداً للقوة الإلكترونية الأمريكية، بما يمكن استكشاف مدى فعالية استخدامها من جانب الولايات المتحدة في إدارة تفاعلاتها الدولية.

حيث يتم على التوالي تناول كل من العوامل القانونية والمؤسسية والفنية والسياسية المؤثرة على استخدام القوة الإلكترونية الأمريكية على النحو التالي:

قدرة الولايات المتحدة الأمريكية على تعظيم قوتها الإلكترونية ليست مطلقة، فهناك قيود تحد منها، سواء كانت هذه القيود قانونية أو مؤسسية أو فنية أو سياسية، فالتسريبات حول التجسس الأمريكي على بعض البلدان الأوروبية، دفعتها للتفكير في إنشاء شبكة اتصالات خاصة بها منفصلة عن الشبكة الأمريكية، فالولايات المتحدة الأمريكية تعمل في عالم إلكتروني يتسم بالتنافسية في مجال القرصنة وأمن المعلومات.

أولاً: العوامل القانونية:

تبرز مشكلة الفضاء الإلكتروني من الناحية القانونية في خصائصه نفسها، فهو عابر للحدود والقوميات والأفكار، ومن ثم يصعب إخضاعه للقانون الوطني، كما أن هناك صعوبة في معرفة الفاعل فيه بسبب خاصية التخفي، فيصعب إخضاعه للقانون الدولي، فضلاً عن كونه يتميز بالسرعة والتطور التكنولوجي المستمر، وبالتالي يصعب تصميم قانون خاص يحكم التعاملات البشرية على مستوى العالم من خلاله، فإذا كان من السهل وضع قانون عام للبحار والمحيطات والفضاء الخارجي، وتنظيم تعاملات الدول فيها، فإن الأمر ليس كذلك بالنسبة للفضاء الإلكتروني لاختلاف خصائصه، وعلى الرغم من محاولات تقنين الإنترنت فإن الأمر مازال يعاني قصوراً في الصياغة، وصعوبة في التنفيذ.

ويمكن هنا استعراض الحدود القانونية الداخلية والخارجية لاستخدام القوة الإلكترونية الأمريكية فيما يلي:

أ- الحدود التي يفرضها القانون الداخلي:

وقد مرت التشريعات الأمريكية بمرحلتين في هذا الصدد:

- المرحلة الأولى: ما قبل 11 سبتمبر 2001:

عملت الولايات المتحدة منذ البداية على تنظيم استخدام وسائل الاتصالات من خلال إصدار القوانين والتشريعات اللازمة لذلك، ووضعت النصوص القانونية التي تحمي الخصوصية الفردية على الإنترنت وتضمن حريات الرأي والتعبير وتراعي السلامة العامة وتحافظ على الأمن القومي الأمريكي. فوضعت قوانين للاتصالات

وأخرى للمعلومات وغيرها للشبكات[1]، وهو الأمر الذي أدى إلى تداخل القوانين ووجود بعض الثغرات فيها، مما يحد حرية الحكومة الأمريكية في ممارسة نفوذها عبر الفضاء الإلكتروني، كما أن الصياغة الدقيقة والواضحة للقوانين بما يتلاءم مع الدستور الأمريكي، تفقد قيمتها مع سرعة التطور الفني والتكنولوجي في عالم الاتصالات والمعلومات.

- المرحلة الثانية: ما بعد 11سبتمبر 2001:

وفي هذه المرحلة تغيرت المنظومة الأمنية في الولايات المتحدة، وخضعت جميع الاتصالات السلكية واللاسلكية للمراقبة بموجب المادة 215 من قانون الأمن الوطني الصادر بعد أحداث الحادي عشر من سبتمبر لمكافحة الإرهاب، الذي سمح لسلطات الأمن بالحصول على تسجيلات الاتصالات التي تتم عبر البريد الإلكتروني من الشركات التي تقدم خدمات الإنترنت[2]، فضيقت على الحريات الشخصية، واقتحمت الخصوصية الفردية، بدواعي مكافحة الإرهاب.

وقد أجرت الولايات المتحدة تعديلات على قانون مراقبة أنشطة الاستخبارات الأجنبية في عام 2007 وتمت تسميته قانون حماية أمريكا Protect America Act، بهدف مراقبة وسائل الاتصالات الإلكترونية، وأنشئت بموجب القانون محكمة عسكرية سرية، هدفها مراقبة أنشطة التجسس الخارجية، وبموجب المادة 702 من القانون تطلب وكالة الأمن القومي الأمريكي من الشركات الأمريكية العاملة في مجال الاتصالات والإنترنت الحصول على المعلومات الاستخباراتية الأجنبية فيما يتعلق بأهداف أجنبية تقع داخل أو خارج الولايات المتحدة تحت إشراف المحكمة[3].

1-Cyberspace Policy Review,**Op Cit**, p P10.
2-**Section 215 of the USA PATRIOT Act,**October 2001, on https://www.eff.org/foia/section-215-usa-patriot-act
3- **The Protect AmericaAct,** Department Of Justice**,** 2007, On http://www.justice.gov/archive/ll/

وقد كشفت بعض تسريبات سنودن عن صدور قرار من المحكمة في أكتوبر 2011 يأمر وكالة الأمن القومي بوقف "برنامج"[1]، لاعتراض الاتصالات الإلكترونية على شبكات الألياف البصرية الأميركية، وكتب جون بايتس القاضي في محكمة مراقبة الاستخبارات الأجنبية أن البرنامج الذي طبقته وكالة الأمن القومي "أدى إلى حصولها على عدد كبير جداً من الاتصالات التي يحميها التعديل الرابع" للدستور الذي يحمي الأميركيين من أي عملية تفتيش أو مراقبة مبالغ فيها[2].

ب- الحدود التي يفرضها القانون الدولي:

على الرغم من عدم وجود سلطة قانونية عليا مباشرة تحكم استخدام الفضاء الإلكتروني، أو تمنع ممارسة أنشطة التجسس على الدول من خلاله، فإن هناك بعض الاتفاقيات والمعاهدات الدولية التقليدية التي تمنع أو تنظم عملية التجسس التقليدية، ويمكن أن ينسحب عليها تشريعياً ممارسة هذا النوع من التجسس عبر الإنترنت، وإذا كانت قواعد الحرب التقليدية لا تنطبق حرفياً على الحرب الإلكترونية عند صياغة اتفاقيات جنيف عام 1949، لكن لايزال القانون الدولي الإنساني منطبقاً على كافة الأنشطة التي تقوم بها الأطراف أثناء النزاع المسلح وينبغي احترامه. ولا يمكن مع ذلك استبعاد حقيقة مؤداها أنه قد تكون ثمة حاجة إلى تطوير القانون لضمان توفيره الحماية الكافية للسكان المدنيين لمواكبة تطور التكنولوجيا أو كلما اتضح تأثيرها الإنساني بشكل أفضل، **ويتضح ذلك في التالي:**

1- لم تتم تسمية هذا البرنامج، ولكن يعتقد الباحث أنه برنامج Wind Stellar الذي تم إيقافه عام 2011، واستبدلته إدارة أوباما ببرامج أقوى وأكثر قدرة على جمع المعلومات.

2- إدارة أوباما تقرب أن وكالة الأمن القومي انتهكت قانون مراقبة الاتصالات، **موقع إيلاف**، بتاريخ 6 سبتمبر 2013، بتاريخ مطالعة 28 أغسطس 2014،يمكن المطالعة على:
http://www.elaph.com/Web/news/2013/8/831530.html#sthash.JweuZei0.dpuf

1- القانون الدولي الإنساني:

بينما لا تذكر اتفاقيات جنيف وبروتوكولاتها الإضافية بشكل محدد الحرب الإلكترونية أو الهجمات عبر شبكة الحاسوب، فإن المبادئ والقواعد التي تتضمنها هذه المعاهدات التي تنظّم سبل وأساليب القتال، لا تنحصر فقط في الحالات التي كانت معروفة في فترة اعتمادها، حيث يستبق القانون الدولي الإنساني بوضوح تام التقدم المحرز في تقنيات صنع الأسلحة وتطور سبل وأساليب جديدة في شن الحروب.

فالقانون الدولي الإنساني لا ينظم العمليات الإلكترونية التي تقع خارج سياق النزاع المسلح، ولكن إذا كان هناك حالة نزاع وتسببت هجمات إلكترونية في تدمير بنى تحتية ألحقت ضرراً بالمواطنين السلميين، كاضطراب أنظمة المواصلات أو المستشفيات ووقوع خسائر في الأرواح البشرية، فإن القانون الدولي الإنساني يجد مساره الطبيعي، وامتثالاً لقواعد القانون الدولي الإنساني، ينبغي ألا تكون هذه الهجمات عشوائية وأن تميّز بين الأهداف العسكرية والمدنيين وتكون متناسبة ومبررة من ناحية الفائدة العسكرية، لذا، لا تختلف تقنيات الحرب الإلكترونية في هذه المجالات، اختلافاً كبيراً عن غيرها من وسائل الحرب، لكنه يُخشى من إمكانية استخدامها، على سبيل المثال، ضد نُظم الإنتاج المدني والتوزيع والنظام المصرفي لدى العدو[1].

ولقد طالبت الدول الأطراف في اتفاقيات جنيف أثناء المؤتمر الدولي الثامن والعشرين للصليب الأحمر والهلال الأحمر المنعقد عام 2003 بأن تخضع جميع الأسلحة ووسائل وأساليب الحرب الجديدة "لاستعراض دقيق ومتعدد التخصصات" وذلك لضمان ألا يتخطى تطور التكنولوجيا الحماية القانونية المكفولة، ويُعَد استخدام العمليات الإلكترونية أثناء النزاعات المسلحة مثالاً جيداً على هذا التطور التكنولوجي السريع[2].

1- الحرب الإلكترونية، **موقع اللجنة الدولية للصليب الأحمر**، بتاريخ دخول 29 أغسطس 2014.
http://www.icrc.org/ara/war-and-law/conduct-hostilities/information-warfare/overview-information-warfare.htm

2- لورانجيسيل، قانون الحرب يضع قيودًا على الهجمات السيبرانية أيضاً، **موقع اللجنة الدولية للصليب الأحمر**، بتاريخ 1 يوليو 2013، بتاريخ دخول 30 أغسطس 2014،

2- دليل تالين:

أعدت لجنة من الخبراء في حلف شمال الأطلسي الناتو دليلاً باسم "دليل تالين"[1] صدر في عام 2013 وخاص بالقوانين الدولية المطبقة في حالة نشوب حروب إلكترونية وتنظيم قواعد الاشتباك عبر الإنترنت، ويشير "دليل تالين" إلى أن القانون الدولي الإنساني ينطبق على الحرب الإلكترونية، ويحدد الدور الذي ستلعبه قواعد القانون الدولي الإنساني في هذا المجال، ويُعَد "دليل تالين" وثيقة غير ملزمة أعدتها مجموعة الخبراء، حيث يقر الدليل بأن العمليات الإلكترونية وحدها قد تشكل نزاعات مسلحة تبعاً للظروف – لاسيما الآثار المدمرة لتلك العمليات – ويقدم الدليل في هذا الصدد تعريفاً "للهجوم الإلكتروني" بموجب القانون الدولي الإنساني بوصفه "عملية إلكترونية، سواء هجومية أو دفاعية يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الإضرار بأعيان أو تدميرها"[2]، وعلى الرغم من عدم إلزامية الدليل، فإنه وثيقة ولو أخلاقية للدول الأعضاء في الحلف على الأقل، لتنظيم استخدامهم للهجمات الإلكترونية خلال فترات النزاع.

3- تحالف الخمس أعين The Five Eyes Network:

في أعقاب الحرب العالمية الثانية، وتحديداً عام 1946 تم توقيع معاهدات ثنائية، أُنشئ بموجبها تحالف مكون من خمس دول هي "الولايات المتحدة الأمريكية والمملكة المتحدة ونيوزيلاندا وأستراليا وكندا"، بهدف مراقبة أنشطة الاتحاد السوفييتي والكتلة الشرقية، وتبادل المعلومات الاستخباراتية بين هذه الدول، من

---

http://www.icrc.org/ara/resources/documents/interview/2013/06-27-cyber-warfare-ihl.htm

1- **دليل تالين حول القانون الدولي المنطبق على الحرب الإلكترونية** – من إعداد اللجنة الدولية للخبراء بدعوة من مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي (الناتو)، مطابع جامعة كامبريدج 2013.

2- Michael N. Schimitt, Editor, **Talinn Manual on the international law applicable to cyber warfare**, Prepared by the international group of experts at the initiative of NATO cooperative cyber defense of excellence, (Cambridge University Press, 2013).

دون تجسسها على بعضها البعض[1]، وهو ما يضع قيداً قانونياً على قدرة الولايات المتحدة على التجسس على أحد من هذه الدول بموجب الاتفاقيات التي تم توقيعها.

ثانياً: العوامل المؤسسية:

ويقصد بها العلاقة بين المؤسسات التنفيذية والتشريعية داخل الولايات المتحدة الأمريكية، والتي قد تصبح عائقاً أمام تحقيق الأمن الإلكتروني الأمريكي.

يمكن التمييز بين نوعين من الحدود المؤسسية:

أ- حدود مؤسسية متعلقة بطبيعة الدولة:

لما كان النظام الأمريكي هو نظام فيدرالي بالأساس يقوم على وجود سلطتين، واحدة فيدرالية اتحادية وأخرى محلية، جاءت المبادرات والاستراتيجيات الوطنية لتؤكد أن مسؤولية الحفاظ على الأمن القومي الأمريكي لم تعد مسؤولية الحكومة الفيدرالية فقط، بل تشاركها أيضاً الحكومات المحلية، بالإضافة إلى القطاع الخاص والمواطنين، ومن هنا يجب التمييز بين الفيدرالي والمحلي عند توزيع المهام والقيام بالواجبات حتى لا تتداخل الاختصاصات أو يتم إغفال بعض المهام، وهو ما يصعب تنفيذه عملياً.

فإذا كان القانون إدارة أمن المعلومات الفيدرالي[2]، قد خول الحكومة الفيدرالية سلطة إنشاء مكاتب فيدرالية لحماية الأجهزة الفيدرالية من الاختراقات والتلاعب

1- Nick Perry And Paisley Dodd**, 5 Nation Spy Alliance Too Vital For Leaks To Harm**, AP, Accessed date August 29th, 2014.
http://bigstory.ap.org/article/experts-say-us-spy-alliance-will-survive-snowden-
2-Federal Information Security Management Act
ويعني قانون إدارة أمن المعلومات الفيدرالي ويتطلب وكالات اتحادية أمريكية لتطوير وتوثيق وتنفيذ برنامج على نطاق الوكالة لتوفير أمن معلومات عن المعلومات (ونظم المعلومات) التي تدعم عمليات الأصول للوكالة.

بالبيانات[1]، فإن القوانين الجنائية الخاصة بالجريمة الإلكترونية قد أعطت سلطات للحكومات المحلية لمواجهة هذا النوع من الجرائم، ولما كانت شبكة الإنترنت مرتبطة إلكترونياً، فإنه لا يمكن فصل الأجهزة المحلية عن تلك الفيدرالية – إلا الأجهزة التي تشكل شبكة داخلية وليست متصلة عبر الفضاء الإلكتروني–، ومن ثم فإن اختراق الأجهزة المحلية يعني بالتبعية إمكانية اختراق الأجهزة الفيدرالية، والعكس صحيح، فهي شبكة واحدة تدار عبر ألياف ضوئية، وبالتالي يصعب عملياً التمييز بين ما هو فيدرالي وبين ما هو محلي.كما أن القوانين التي تعاقب على الجرائم الإلكترونية أو محاولة استخدام الإنترنت في أغراض غير سلمية، تأتي كرد فعل بهدف معاقبة الجاني، وليس ضمن خطوط الدفاع الأولية الاستباقية التي تمنع وقوع الجريمة منذ البداية، ومن ثم فإن هذه القوانين لا تتلاءم مع هذه المبادرات والاستراتيجيات الطموحة التي تسعى لكشف الجريمة أو الهجوم الإلكتروني قبل وقوعه، بل بالعكس، تعسى لاستغلال الهجمات الإلكترونية المضادة لاختراق شبكات العدو أثناء محاولاته اختراق الأجهزة الأمريكية.

ب- حدود مؤسسية متعلقة بنظام الحكم:

يتميز النظام الأمريكي بالفصل بين السلطتين التنفيذية والتشريعية، وقد أعطى الدستور الأمريكي سلطات لكل من البرلمان ورئيس الجمهورية، فيحق للبرلمان إعلان حالة الحرب والتعبئة العامة للجنود ووضع قواعد منظمة لعمل القوات المسلحة الأمريكية، وفي الوقت نفسه جعل الرئيس الأمريكي هو القائد العام للقوات المسلحة، فيحين لا يمكن أن يتولى عضو بالكونجرس الأمريكي مسؤولية وزارة في الحكومة إلا بعد تقديم استقالته، وهو ما قد يؤدي إلى حدوث خلاف في وجهات النظر خاصة إذا كان رئيس الدولة من حزب أغلبية والكونجرس الأمريكي من حزب آخر، وقد سبق وحدث خلاف بين الحكومة والكونجرس أبرزها حينما أصر النواب الجمهوريون على

1- **Federal Information Security Management Act (Fisma) Implementation Project**, Accessed Date, August30th, 2014, on http://csrc.nist.gov/groups/SMA/fisma/

تأجيل إصلاحات الرعاية الصحية التي تبناها الرئيس أوباما الذي ينتمي للحزب الديمقراطي كشرط لإقرار ميزانية العام الجديد[1]، وظلت الميزانية الجديدة معلقة بيد الكونجرس، وهو ما دفع البيت الأبيض إلى إصدار أوامره إلى دوائر الحكومة الفيدرالية بوقف جزئي للعمل فيها بعدما أخفق الكونجرس في التوصل الى اتفاق حول هذه الأزمة، وقد نشب عنها توقف بعض خدمات الحكومة الأمريكية لمدة 16 يومياً[2]، وقد أصاب هذا التوقف أيضاً بعض مواقع الإنترنت الحكومية مثل موقع البيت الأبيض ووكالة الفضاء الأمريكية ناسا وغيرها.

وعلى غرار هذا الخلاف، قد ينشب أيضاً خلاف حول الاعتمادات المالية المخصصة للأمن الإلكتروني في الميزانية الأمريكية، وعلى الرغم من عدم حدوث هذا الأمر خلال فترة الدراسة، فإنه يظل أحد الاحتمالات القائمة حول أولوية توجيه أموال الميزانية الأمريكية مستقبلاً، مما يضع حدوداً حول قدرة المؤسسة التنفيذية على القيام باستراتيجياتها المنشودة بسبب عدم موافقة الكونجرس على التمويل.

ولما كانت رقابة الكونجرس الأمريكي تمتد لتشمل بعض أنشطة المخابرات السرية والمهمة، بالقدر الذي يسمح بعدم الكشف أو تسريب معلومات حول هذه المهام، فإنه إذا قرر الرئيس اتخاذ بعض القرارات السرية والضرورية لمواجهة ظروف غير عادية يمكن أن تؤثر على المصالح الحيوية للولايات المتحدة، فإن اتخاذ هذا القرار لابد أن يحظى بموافقة عدد ولو قليل من زعماء الكونجرس.

1- أزمة الميزانية الأمريكية: إغلاق دوائر حكومية فيدرالية بسبب الخلاف، **موقع BBC**، تاريخ 17 نوفمبر 2013، مطالعة بتاريخ 17 نوفمبر 2013.

http://www.bbc.co.uk/arabic/worldnews/2013/10/131001_us_budget_shutdown.shtml

2- تأجيل معركة رفع سقف الدَّين وإغلاق الحكومة الأمريكية، **موقع جريدة الاقتصادية**،18 أكتوبر 2013، بتاريخ دخول 17 نوفمبر 2013،

http://www.aleqt.com/2013/10/18/article_793563.html

ثالثاً: العوامل الفنية:

وتشمل عدداً من التحديات أبرزها التي تواجهها حكومة الولايات المتحدة وتتمثل في التالي:

أ- تطوير برامج دفاعية:

هناك معركة مشتعلة دائماً بين صناع الفيروسات من جهة وشركات البرمجيات من جهة أخرى، فحينما ظهرت فيروسات الكمبيوتر واتضحت خطورتها، بدأت شركات البرمجة إنتاج برامج مضادة لها، تعمل على إزالتها ووقف نشاطها، وهو ما استثار صانعي الفيروسات، فقاموا بإنتاج فيروسات أكثر ضراوة وأخطر انتشاراً، إلى الحد الذي أصبح الفيروس فيه يمكنه إصابة المكون المادي للأجهزة الإلكترونية وإصابتها بالشلل، وليس فقط تدمير برنامج التشغيل، كما أن تطوير أساليب وأنظمة أمن المعلومات يكون غالباً رد فعل على هجمات إلكترونية ناجحة، ومن ثم تظهر الثغرات التي تم ارتكاب هذه الهجمات منها، وتبدأ مرحلة تأمينها، ولذلك كان من الضروري القيام بأساليب محاكاة لشن هجمات إلكترونية لمعرفة مواطن الضعف وتلافيها، وهو الأمر الذي دفع الولايات المتحدة للقيام سنوياً بمحاكاة للتعرض لحرب إلكترونية فيما يطلق عليه Cyber Storm أو عاصفة الحواسب لمواجهة هذه التهديدات الإلكترونية، وهو ما يتطلب أموال طائلة وميزانيات مخصصة لأغراض الحرب الإلكترونية واستمرار تحقيق الريادة التكنولوجية.

وتكمن التحديات الفنية في صعوبة مراقبة وتأمين كل ما هو مرتبط بالفضاء الإلكتروني، فالأمر لا يقتصر على الحاسب الآلي فقط بل امتد ليشمل الهاتف المحمول والتليفزيون الذكي والحاسب اللوحي (Tablet)، وأصبح الفضاء الإلكتروني عنصراً رئيسياً في معظم الأجهزة الإلكترونية الحديثة، بل يتم حالياً وضع مئات الآلاف من التطبيقات والبرامج على الهاتف المحمول، وهو ما يعني مئات الآلاف من الهجمات الإلكترونية المحتملة، وهو أمر يصعب تأمينه، ومن ثم فهناك صعوبات جمة تواجه

استراتيجيات الأمن الإلكتروني الأمريكية، بسبب الصراع الحتمي والمحتدم بين صناعة القرصنة وصناعة أمن المعلومات.

ب- حماية حقوق الملكية الفكرية وبراءات الاختراع:

ولعل من أبرز التهديدات الإلكترونية التي تواجه الولايات المتحدة انتهاك الملكية الفكرية، خاصة في الصناعات الحيوية والاستراتيجية، من خلال سرقة البيانات والمعلومات والتكنولوجيا الأمريكية إلكترونياً، والعمل على الاستفادة منها وتطويرها، وهو الأمر الذي تسبب في خسائر كبيرة للصناعات الاستراتيجية، كما أن الأمر امتد ليشمل أسرار صناعات عسكرية وحربية، حيث استهدف قراصنة إلكترونيون في "شنجهاي" ما لا يقل عن 20 شركة أمريكية تتعامل مع البنتاجون للاستيلاء على الأسرار التكنولوجية التي تقف وراء تفوق الولايات المتحدة الأمريكية في صناعة الطائرات من دون طيار، سواء الحربية أو التجسسية، وذلك في إطار اهتمام الصين بتطوير قدراتها التكنولوجية في هذا المجال، كما اتهمت وزارة الدفاع الأمريكية الصين بأنها تلجأ إلى التجسس للحصول على التكنولوجيا التي تساعدها في تحديث جيشها من خلال محاولة اختراق شبكات الكمبيوتر الدفاعية الخاصة بالولايات المتحدة الأمريكية[1].

ج- التأكد من ولاء العنصر البشري:

وقد مثلت أزمة الويكيلكس نموذجاً على ضعف معايير الأمن الإلكتروني الأمريكي، فقد اهتمت الولايات المتحدة بتأمين الخوادم والمواقع من عمليات القرصنة الإلكترونية، وأهملت العنصر البشري القائم على هذه الخوادم والمواقع، فبمساعدة أحد ضباط الجيش الأمريكي تمكن ويليم أسانج من تسريب ملايين الوثائق السرية الخاصة بوزارة

1- نسرين فوز اللواتي، سباق التسلح التكنولوجي بين أمريكا والصين، **مجلة لغة العصر**، نوفمبر 2013 ،يمكن الطالعة على:
http://digital.ahram.org.eg/Motnw3a.aspx?Serial=1454951&archid=23

الخارجية الأمريكية، وتكرر هذا النموذج بصورة أخرى في وقت سابق، كما قام إدوارد سنودن بتسريب وثائق سرية للغاية إلى صحيفة الجارديان البريطانية، وقد قال وليام لين نائب وزير الدفاع الأميركي "إن جهاز مخابرات أجنبياً سرق 24 ألف ملف من شركة متعاقدة مع وزارة الدفاع الأميركية (البنتاغون) في شهر مارس 2011"، وهو ما يظهر حجم التهديد الذي تواجهه الوزارة وهي تسعى إلى تعزيز أمنها الإلكتروني[1].

د- توفير التمويل اللازم:

تعتمد معظم البنية التحتية الأمريكية على الفضاء الإلكتروني والخدمات الرقمية، وتدير معظم هذه البنى شركات خاصة، ولتأمين البنية التحتية الأمريكية، خاصة المدنية، فإن الأمر يحتاج إلى مليارات الدولارات، حتى لا تقع ضحية لهجمات إلكترونية تتسبب في وقوع خسائر بشرية، هذه الأموال تعجز عن توفيرها الشركات الخاصة، إلا بتدخل ودعم مالي حكومي، وهو ما يطرح معضلة توفير مثل هذا التمويل أمام الحكومة الفيدرالية.

1- استراتيجية البنتاجون لأمنه الإلكتروني، **موقع الجزيرة**،15 يوليو 2011، بتاريخ دخول 28 أغسطس 2014 يمكن المطالعة
http://www.aljazeera.net/news/pages/10d21d07-86fb-401f-940a-6752418f1d2c

رابعاً: العوامل السياسية:

إذا استطاعت الولايات المتحدة أن تتغلب على المشاكل القانونية بإعادة صياغتها وتحديد الاختصاصات والسلطات وفقاً للقانون، وإذا استطاعت أيضاً التغلب على المشاكل والعقبات الفنية والتكنولوجيا لتعظيم قوتها الإلكترونية، فإنه من الصعب تماماً التغلب على الحدود السياسية، سواء داخلياً أو خارجياً، فالمواطنون لن يقبلوا بانتهاك حرياتهم على الفضاء الإلكتروني أو اقتحام خصوصياتهم وتسجيل بياناتهم ومكالماتهم ورسائلهم الإلكترونية إلى أجل غير مسمى بدواعي مكافحة الإرهاب، كما أن مصالح الدول خارجياً تتعارض في بعض الأحيان، مما يجعل قدرة دولة واحدة على زيادة قوتها الإلكترونية وتحقيق الريادة منفردة في هذا المجال أمراً صعب المنال، **ومن ثم يمكن تتبع هذه القيود على المستويين الداخلي والخارجي:**

أ- على المستوى الداخلي:

تمثل الحرية الشخصية أحد أهم المبادئ الرئيسية في النظام السياسي الأمريكي، إلا أن هذا المبدأ لم يجد له مجالاً في الفضاء الإلكتروني، فبقوة القانون، يحق للولايات المتحدة مراقبة وتسجيل بيانات جميع مستخدمي الفضاء الإلكتروني، استناداً إلى مبدأ مكافحة الإرهاب وحماية أمن المواطنين، وهو ما يطرح جدلية العلاقة بين الحرية الشخصية والأمن الشخصي، فزيادة أحدهما تأتي على حساب الآخر، وهو ما يتضح جلياً في اختراق الحريات الفردية على الفضاء الإلكتروني، إلا أن التساؤل يظل موجوداً، إلى متى سيرضى المواطن الأمريكي بانتهاك حريته الشخصية بدواعي مكافحة الإرهاب، ولعل أخطر الوثائق التي سربها إدوارد سنودن هو ما يتعلق بتجسس الولايات المتحدة على مواطنيها، وهو ما برره الرئيس الأمريكي باراك أوباما بمحاولة الحكومة الأمريكية رصد أي محاولات لعمليات إرهابية محتملة.

ب- على المستوى الخارجي:

تشهد دول مجموعة البيركس التي تتكون من "روسيا – الصين – البرازيل- الهند – جنوب أفريقيا"، تطورات تعليمية وتكنولوجية ملحوظة، وهو ما أثارالقلق الأميركي من تزايد المهارات التكنولوجية لهذه المجموعة، فقد حذرت التقارير الصادرة عن جامعة ستانفورد الأميركية[1]، من قدرة بعض بلدان البيركس على منافسة أميركا من خلال جودة تعليم العلوم والتكنولوجيا، وهي دول تسعى إلى خلق أنظمة جامعية على مستوى عالمي، وكما تقوم بضخ موارد كبرى في مؤسسات التعليم العالي.

وقد أثار ما نشر من تقارير عن عمليات التجسس التي قامت بها وكالة الأمن القومي الأمريكية ردود أفعال غاضبة من عدد من الدول الأوروبية، وعلى رأسها ألمانيا، وذلك إثر المعلومات التي أكدت أن رئيسة الوزراء، أنجيلا ميركل، كانت هدفاً لعمليات التجسس منذ عام 2002 وحتى عام 2010، وأن المكالمات الهاتفية التي أجرتها من هاتفها تم تسجيلها طوال هذه المدة[2].

فمن الملحوظ أن هناك حرباً مستعرة وخفية بين الولايات المتحدة الأمريكية والصين على مختلف المجالات السياسية والعسكرية والاقتصادية، حيث أشارت صحيفة الشعب الصينية إلى أنه وفقاً للبيانات التي حصلت عليها وكالة أنباء بلومبرغ نيوز الأمريكية في 14 ديسمبر 2011، فإن هناك 760 مؤسسة أمريكية من بينها شركات وجامعات ومزودي خدمات الإنترنت وهيئات حكومية قد تعرضت لهجمات قراصنة وجواسيس نت صينيين خلال السنوات العشر الماضية، كما أشارت

1- قلق أميركي من تزايد المهارات التكنولوجية لمجموعة البيركس، **موقع جريدة العرب**، تاريخ دخول 14 ديسمبر 2013، يمكن المطالعة على :

http://www.alarab.co.uk/?id=3430

2- نوران شفيق علي،ا لثقة المفقودة: تداعيات أزمة التجسس الأمريكي على الدول الأوروبية، **موقع مجلة السياسة الدولية**، تاريخ دخول 14 ديسمبر 2013،

http://www.siyassa.org.eg/NewsContent/2/100/3343/%D8%AA%D8%AD%D9%84%D9%8A%D9%84%D8%A7%D8%AA/%D8%B4%D8%A6%D9%88%D9%86-%D8%AF%D9%88%D9%84%D9%8A%D8%A9/-%D8%A7%D9%84%D8%AB%D9%82%D8%A9-%D8%A7%D9%84%D9%85%D9%81%D9%82%D9%88%D8%AF%D8%A9.aspx

إلى أن شركات أمريكية كبرى، مثل غوغل وإنتل وشركات عاملة في مجال الطيران والمواصلات والدواء والتكنولوجيا البيولوجية كانت هدفاً لهجمات قراصنة النت الصينيين[1]، وعلى الرغم من صعوبة معرفة مصدر الهجمات، فإنها تبقى عائقاً أمام الطموحات الأمريكية الإلكترونية.

ونخلص مما سبق لنتيجة مفادها، أن قدرة الولايات المتحدة الأمريكية على تعظيم قوتها الإلكترونية ليست مطلقة، فهناك قيود تحد منها، سواء كانت هذه القيود قانونية أو مؤسسية أو فنية أو سياسية، وأن الولايات المتحدة تعمل في عالم إلكتروني يتسم بالتنافسية في مجال القرصنة وتأمين المعلومات.

1- أمريكا تتهم الصين بشن "حرب إنترنت باردة، **موقع الشعب الصيني**، بتاريخ دخول 23 مايو 2014، يمكن المطالعة على:
"http://arabic.people.com.cn/102267/102268/7679611.html

الخلاصة:

نخلص من هذا الفصل إلى أن هناك تغيراً في طبيعة التهديدات الإلكترونية التي تواجهها الولايات المتحدة، من الاكتفاء باستعراض مظاهر قوة الخصم باختراق مواقع أو غلق مواقع، إلى سرقة البيانات والسعي لاختراق البنى التحتية كشبكات الطاقة والكهرباء، وهو ما يمثل خطراً حقيقياً على الأمن القومي الأمريكي.

ولمواجهة هذه المخاطر قامت الولايات المتحدة بإعداد مجموعة من الخطط والاستراتيجيات التي تسعى لتأمين الفضاء الإلكتروني، واعتباره مسرحاً لعمليات عسكرية ممكنة، وهو ما يطرح فكرة جديدة وهي "عسكرة الفضاء الإلكتروني"، على أن كل هذا لم يمنع من أن تتعرض مواقع الإدارة الأمريكية لآلاف الهجمات الإلكترونية، مع نجاح العديد من هذه الهجمات بتحقيق أهدافها المتمثلة، إما في إيذاء الشبكات والأنظمة الكمبيوترية الحكومية الأميركية، أو بالتسلل إلى البيانات المخزنة فيها والاطلاع على هذه البيانات، وبعضها بالغ السرية ويتعلق بمسائل الأمن القومي الأميركي.

وهو ما يطرح العديد من التساؤلات إزاء فعالية التدابير المتخذة والتشريعات الصادرة بهذا الصدد، على أن هذا التعدد والتنوع في المبادرات والمكاتب والوكالات ينمّ في الحقيقة عن حالة من الفوضى وعدم التنسيق للتصدي للاعتداءات المعلوماتية هناك، ما يفسر أمر تواصل تعرض الولايات المتحدة لهذا النوع من الاعتداءات، هذا فضلاً عن وجود عوامل سياسية وفنية تمثل قيوداً على القوة الإلكترونية الأمريكية.

الفصل الثالث

تطبيقات لاستخدام القوة الإلكترونية الأمريكية

في التفاعلات الدولية خلال رئاستي بوش وأوباما

استعرضنا خلال الفصلين السابقين الاستخدامات النظرية للقوة الإلكترونية، سواء على مستوى القوة الصلبة أو الناعمة، وتطرقنا إلى مصالح وتهديدات الولايات المتحدة في الفضاء الإلكتروني، والعقيدة التي تحكم الولايات المتحدة في استخدام القوة الإلكترونية، وقد تم التأكيد على أن القوة الإلكترونية أصبحت عنصراً حاكماً ومحدداً للاستراتيجية العسكرية الأمريكية، حيث يُنظر للفضاء الإلكتروني على اعتبار أنه مجال لعمليات عسكرية محتملة، وفيما يلي نتطرق إلى جزء تطبيقي يوضح كيف تدير الولايات المتحدة تفاعلاتها السياسية والعسكرية والاقتصادية من خلال القوة الإلكترونية، والتفاعلات هنا تشمل اتجاهين من وإلى الولايات المتحدة الأمريكية.

وتتعدد استخدامات القوة الإلكترونية في إدارة التفاعلات الدولية، وتختلف الآلية التي تدير بها الولايات المتحدة تفاعلاتها وفقاً لطبيعة الظروف الدولية المحيطة، ومن ثم يحاول الكاتب في المبحث الأول الخروج بنمط pattern يعكس استخدام الولايات المتحدة لهذه القوة في إدارة تفاعلاتها السياسية والعسكرية، وكيف أثرت هذه القوة سواء بالإيجاب أو السلب على الولايات المتحدة، ويسعى الكاتب في المبحث الثاني إلى الوقوف على الاستخدامات الاقتصادية للقوة الإلكترونية في إدارة التفاعلات الدولية بين الولايات المتحدة الأمريكية ومختلف القوى الاقتصادية الدولية.



المبحث الأول

استخدام القوة الإلكترونية الأمريكية في التفاعلات الدولية السياسية

لا تتوانى الولايات المتحدة الأمريكية عن استخدام القوة الإلكترونية في إدارة تفاعلاتها الدولية، السياسية والعسكرية، بما يساعد في تعظيم قوة الولايات المتحدة وتحقيق أهدافها التي تعجز أدوات القوة التقليدية عن تحقيقها، خاصة بما تتميز به هذه القوة من خاصية التخفي والقدرة على إصابة أهداف الخصم، واتساع نطاق تدمير الأهداف الإلكترونية مع التحكم في إمكانية إصابة الأهداف من دون وقوع خسائر بشرية غير مقصودة.

ويعد اللجوء إلى القوة الإلكترونية لإدارة التفاعلات السياسية من الطرق غير التقليدية التي يمكن أن تحقق بها دولة ما أهدافها وأن ترسل رسائل من خلالها، ومن خلال دراسة تفاعلات الولايات المتحدة السياسية خلال فترة الدراسة والوقوف على استخدامات القوة الإلكترونية فيها.

لاحظ الكاتب أن توظيف القوة الإلكترونية لتحقيق أهداف سياسية يتمثل في الأنماط التالية:

تتنوع استخدامات الولايات المتحدة لقوتها الإلكترونية في إدارة تفاعلاتها السياسية، بين التجسس وسرقة المعلومات السياسية والاستراتيجية، وبث رسائل عبر مواقع التواصل الاجتماعي، بالإضافة إلى تدعيم المعارضة السياسية عبر الفضاء الإلكتروني واتباع نمط جديد من الدبلوماسية قائم على الانترنت هو الدبلوماسية الإلكترونية، وتطوير طرق لمواجهة الحركات المتطرفة والإرهابية عبر الفضاء الإلكتروني.

1- الاستخبارات الإلكترونية Cyber Intelligence:

من المعروف أن جميع الدول تحاول التجسس على بعضها البعض لتحقيق أمنها القومي ومصالحها الاستراتيجية، وهو شيء تقليدي ومعروف عبر التاريخ، ولكن الثورة التي أحدثتها التكنولوجيا الحديثة طورت طرق التجسس، فأصبح بالإمكان التجسس على ملايين الأفراد في الوقت نفسه، وتسجيل مكالماتهم الهاتفية، وصورهم الشخصية، ومراسلاتهم البريدية، بل وتصوير حياتهم الشخصية لحظة بلحظة، مما جعل الصعوبة الرئيسية ليست في التجسس، ولكن في كيفية إدارة المعلومات العملاقة Mega Data الناجمة عن عملية التجسس، وقد كشفت تسريبات سنودن عن أكبر عمليات تجسس قامت بها الولايات المتحدة، والتي شملت التجسس على جميع دول العالم باستثناء 4 دول هي بريطانيا واستراليا وكندا ونيوزيلاندا[1]، وقد أشارت صحيفة الواشنطن بوست إلى أن هناك ترخيصاً قانونياً سرياً يعود تاريخه إلى عام 2010، وغيره من الوثائق تثبت أن لوكالة الأمن القومي الأمريكي صلاحيات واسعة وأساليب مرنة سمحت لها بأن ترصد من خلال شركات أمريكية، ليس فقط اتصالات لأهدافها في الخارج، بل أي اتصالات محيطة بتلك الأهداف.

وفيما يلي بعض هذه النماذج التي تسببت في أزمات دبلوماسية للولايات المتحدة خلال فترة الدراسة:

- حدثت أزمة دبلوماسية بين الولايات المتحدة الأمريكية وجمهورية ألمانيا الاتحادية على خلفية مزاعم بقيام وكالة الأمن القومي الأمريكي بالتجسس على هاتف المستشارة الألمانية إنجيلا ميركل منذ عام 2002[2]، حيث استدعى وزير الخارجيةُ الألماني غيدوفيسترفيلي السفير الأميركي لأول مرة في تاريخ البلدين منذ

1-Court gave NSA broad leeway in surveillance, **Washington Post**, documents show, June 30, 2014, Accessed on July 3, 2014, http://www.washingtonpost.com/world/national-security/court-gave-nsa-broad-leeway-in-surveillance-documents-show/2014/06/30/32b872ec-fae4-11e3-8176-f2c941cf35f1_story.html

2- تقرير: الولايات المتحدة تجسست على هاتف ميركل منذ 2002، **موقع BBC**، تاريخ 26 أكتوبر 2013، بتاريخ دخول 19 أبريل 2014، يمكن المطالعة على:
http://www.bbc.co.uk/arabic/worldnews/2013/10/131026_us_bugged_merkel.shtml

الحرب العالمية الثانية، لطلب توضيحات بشأن المعلومات التي أفادت بأن أجهزة الاستخبارات الأميركية ربما تجسست على الهاتف المحمول للمستشارة أنجيلا ميركل[1]، وقد اعتذر الرئيس الأمريكي باراك أوباما للمستشارة الأمريكية، مؤكداً أنه لم يكن يعرف بوقوع هذا التجسس، وأنه كان سيمنعه حال عرفه[2].

- وبالمثل استدعى وزير الخارجية الفرنسي لوران فابيوس السفير الأمريكي في باريس لمناقشة تقرير نشرته صحيفة فرنسية يقول إن الولايات المتحدة تجسست على ملايين المكالمات الهاتفية الخاصة بالمواطنين في فرنسا، كما ذكرت تقارير صحفية أن وكالة الأمن القومي الأمريكية تجسست على دبلوماسيين فرنسيين في واشنطن وفي الأمم المتحدة[3].

- وقد نشرت صحيفة الجارديان البريطانية تقريراً حول قيام الموظف السابق إدوارد سنودن بوكالة السي آي إيه، بتسريب وثائق سرية إلى الصحفي الأمريكي جلين جرنوالد الذي يقيم في ريو دي جنيرو ويراسل صحيفة الجارديان، والتي تكشف أن وكالة الأمن القومي قامت بمراقبة هاتف رئيسة البرازيل ديلما روسيف ورسائل بريدها الإلكتروني التي تتبادلها مع مستشاريها ووزرائها[4]، مما دفع الرئيسة البرازيلية، الي إلغاء زيارتها التي كانت مقررة للولايات المتحدة يوم 23 أكتوبر 2012، ولم تكتف بذلك بل انتقدت في الجلسة الافتتاحية للجمعية العامة للأمم المتحدة ما قامت به حكومة الولايات المتحدة من تجسس على بلادها وعليها شخصياً من خلال شبكة الإنترنت, خاصة في حضور الرئيس الأمريكي، الذي ألقى

1- برلين تستدعي السفيرالأميركي حول التجسس على ميركل، **موقع العربية**، 24 أكتوبر 2013،19 أبريل 2014،يمكن المطالعة على،

http://www.alarabiya.net/ar/arab-and-world/2013/10/24

2- أوباما لم يكن على علم بـ"التجسس على هاتف ميركل"،**على موقعBBC**، بتاريخ 19 أبريل 2014، بتاريخ دخول 19 أبريل 2014،يمكن المطالعة على:

:http://www.bbc.co.uk/arabic/worldnews/2013/10/131027_obama_merkel_phone_spy_row.shtml

3- فرنسا تستدعي السفير الأمريكي في باريس لمناقشة تهم بالتجسس على ملايين الفرنسيين، **موقع BBC**، بتاريخ 13 أكتوبر 2013بتاريخ دخول 19 أبريل 2014، يمكن المطالعة على:

http://www.bbc.co.uk/arabic/worldnews/2013/10/131021_france_us_spying_crisis.shtml

4-Brazil demands explanation from US over NSA spying, **The Guardian,**On July 8th, Accessed on April 19th, 2014, On

http://www.theguardian.com/world/2013/jul/08/brazil-demands-explanation-nsa-spying

كلمته بعدها مباشرة، وتعمد فيها الإشارة بشكل مقتضب إلى سيل الانتقادات التي وجهته له ولحكومته, وأبدى دفاعاً عن فعالية برنامج التنصت الأمريكي، الذي قال إنه كان السبب في جعل العالم أكثر استقراراً مما كان عليه قبل خمسة أعوام، كما بررت الإدارة الأمريكية عمليات التجسس بأن الهدف منها هو الكشف عن أي عملية إرهابية قبل وقوعها، وكان أيضاً من بين تبعات الكشف عن التجسس على البرازيل، أن تم تعليق المفاوضات مع الولايات المتحدة حول صفقة قيمتها أربعة مليارات يورو لشراء طائرات متعددة الأدوار[1].

- ومن ناحية أخرى وإبان الانتخابات الرئاسية الأمريكية 2008 قامت مجموعة من القراصنة المجهولين باختراق قواعد البيانات الخاصة بالحملتين الرئاسيتين للحزب الجمهوري والديمقراطي وتنزيلها[2].

1- شريف الغامري، أمريكا تتجسس علي العالم!، **موقع الأهرام**، بتاريخ دخول 19 أبريل 2014، يمكن المطالعة على:
http://www.ahram.org.eg/NewsPrint/236114.aspx

2- تاريخ الهجمات الإلكترونية، **مجلة حلف الناتو**، تاريخ مطالعة 18 أبريل 2014، يمكن المطالعة على:
http://www.nato.int/docu/review/2013/Cyber/timeline/AR/index.htm-

2- بث رسائل عبر شبكات التواصل الاجتماعي:

لعبت مواقع التواصل الاجتماعي دوراًمهماً خلال ثورات الربيع العربي، فكانت نموذجاً على تحول الحشد الافتراضي إلى حشد على أرض الواقع، وانتقلت من مرحلة التأثير الافتراضي، إلى مرحلة التأثير الواقعي، مما أكسب هذا النوع من المواقع أهمية كبيرة في التأثير على الأحداث السياسية، وأصبحت من القنوات الرسمية التي يستخدمها القادة السياسيون للتعبير عن آرائهم.

وقد نشرت صحيفة الجارديان في مارس 2011 تقريراً حول قيام الجيش الأمريكي بتطوير برنامج إلكتروني يدعى Sock Puppet، يعمل على تدشين حسابات شخصية على مواقع التواصل الاجتماعي بلغات مختلفة، بهدف بث رسائل تدعم الرؤية الأمريكية على مواقع التواصل الاجتماعي، حيث يقوم أحد الأشخاص بالتحكم في 10 حسابات شخصية غير حقيقية على مواقع التواصل وفي مناطق مختلفة من العالم، وهو ما يمكن الولايات المتحدة من خلق اتجاه عام مزور نحو قضايا معينة في مواقع التواصل الاجتماعي، يمكن أن يؤثر في الأحداث السياسية[1].

كما أعلنت وكالة مشاريع البحوث الدفاعية المتطورة (DARPA) في العام 2011 عن برنامج لاستخدام مواقع التواصل الاجتماعي في تحقيق التواصل الاستراتيجي Social Media In Strategic Communication Program (SMISC) حيث يهدف هذا البرنامج إلى تحقيق هدفين رئيسيين، الأول هو تحسين فهم وزارة الدفاع لما يجري على مواقع التواصل الاجتماعي في الوقت الحقيقي له Real Time، خاصة في المناطق التي تنتشر فيها قوات أمريكية، أما الهدف الثاني، فهو قيام وزارة الدفاع باستخدام مواقع التواصل في بث رسائل إعلامية تخدم مصالحها الاستراتيجية[2].

1-Nick Fielding and Ian Cobain, Revealed: US spy operation that manipulates social media, **The Guardian,** On 21 March 2014,
http://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks
2-**Pentagon Seeks to Manipulate Social Media for Propaganda Purposes**, Global research, On April 21th, 2014, http://www.globalresearch.ca/pentagon-seeks-to-manipulate-social-media-for-propaganda-purposes/25719

وقد كشفت مؤسسة "Digital Policy Council" "مجلس السياسة الرقمية" التي تراقب أنشطة حكومات الدول على موقع تويتر للتواصل الاجتماعي أنه في ديسمبر 2012 كان هناك 123 رئيس دولة يستخدمون موقع تويتر للتواصل مع الجماهير، وقد تصدر الرئيس الأمريكي باراك أوباما قائمة زعماء دول العالم من حيث عدد أعضاء تويتر الذين يتابعون أنشطته على الموقع[1].

1-123 رئيس دولة يستخدمون موقع تويتر للتواصل مع شعوبهم يتقدمهم أوباما وشافيز وجول، **موقع الاهرام**، بتاريخ دخول 21 أبريل 2014، يمكن المطالعة على:

http://gate.ahram.org.eg/NewsContentPrint/25/113/291841.aspx

3- تدعيم المعارضة السياسية الإلكترونية:

يعتبر الفضاء الإلكتروني من ضمن الأدوات التي يمكن من خلالها التعبير عن الرأي، خاصة في ظل النظم السياسية الديكتاتورية التي لا تسمح بحرية الرأي والتعبير، حيث يعتبر الفضاء الإلكتروني مجالاً واسعاً لإنشاء المدونات واستخدام مواقع التواصل الاجتماعي مثل الفيس بوك وتويتر واليوتيوب وغيرها للتعبير عن الرأي، وهو ما يسبب إزعاجاً لبعض النظم السياسية، فتلجأ إلى حبس المدونين الإلكترونيين، أو حجب بعض المواقع الاجتماعية، وعادة ما تستخدم الولايات المتحدة هذه الورقة لتدعيم المعارضة السياسية، أو للدفاع عن حرية التعبير، باعتبارها رائداً لليبرالية السياسية والاقتصادية العالمية، ومن أبرز الأمثلة على ذلك، انتقاد الولايات المتحدة الحكم الصادر من محكمة عسكرية مصرية بسجن المدون مايكل منير ثلاث سنوات بعد أن أسس صفحة على موقع التواصل الاجتماعي فيسبوك تدعو لمناهضة التجنيد الإجباري وكتب عدة مقالات على مدونته الشخصية ينتقد تعامل الجيش مع المطلوبين للتجنيد[1].

وقد تم استخدام الإنترنت في دعم الاحتجاجات الإيرانية على نتيجة الانتخابات الرئاسية في عام 2009 وظهرت الحركة الخضراء المعارضة عام 2009 والتي أُطلق عليها اسم «ثورة تويتر» سواء عبر شبكات التواصل الاجتماعي أو عبر الهاتف المحمول وأدوات الإعلام الجديد ولاقى ذلك دعماً من شركات غربية بتأييد ضمني من الولايات المتحدة[2].

وقد حدثت أزمة بين شركة جوجل الأمريكية والحكومة الصينية في يناير 2010، حيث ادعت أن الحكومة الصينية تقوم باختراق موقعها الإلكتروني بهدف التجسس

1- الولايات المتحدة تدين حبس مدون مصري انتقد الجيش، **موقع راديو سوا**، بتاريخ دخول 26 أبريل 2014، يمكن المطالعة على:

http://www.radiosawa.com/content/article/34782.html#ixzz301Y9KPBI

2- عادل عبدالصادق،الإنترنت والدبلوماسية ومعركة القوة الناعمة بين الولايات المتحدة وإيران، **مجلة مختارات إيرانية**، منشور على موقع الأهرام بتاريخ دخول 28 أبريل 2014، يمكن المطالعة على:
http://digital.ahram.org.eg/articles.aspx?Serial=719287&eid=9723

على حسابات البريد الإلكتروني الخاص بناشطين سياسيين في مجال حقوق الإنسان بالصين، وهو ما يتنافى مع سياسة وخصوصية الشركة، في حين اتهمت الصين شركة جوجل باختراق الاتفاق المبرم بينهم منذ بداية عمل جوجل بالصين عام 2006 بإخضاع هذه العمليات للرقابة، الأمر الذي أدى إلىتسيييس القضية بعد مطالبة الولايات المتحدة الصين بفتح تحقيق في تلك الهجمات ومنع الرقابة على الإنترنت بل والتهديد بالاختصام لدى منظمة التجارة العالمية علي اعتبار ذلك ضد حرية الإنترنت وأن الولايات المتحدة تتحمل المسؤولية في تأمين استخدامه[1].

1- عادل عبد الصادق، الصين وجوجل .. أزمة متعددة الأبعاد، **موقع الأهرام بتاريخ** دخول 18 أبريل 2014، يمكن المطالعة على:

http://www.ahram.org.eg/archive/The-Writers/News/16447.aspx

4- الدبلوماسية الإلكترونية Cyber Diplomacy:

يُشير مفهوم الدبلوماسية بشكله التقليدي إلى "عمليات الاتصال والتفاوض والتمثيل التي تجرى بين الدول بصفة رسمية، لاسيما عن طريق الحكومات". وتختلف عن مفهوم الدبلوماسية العامة Public Diplomacy أو كما يُطلِق عليها البعض "الدبلوماسية الشعبية" كون الأخيرة أشمل وأوسع، حيث تتضمن بجانب ما سبق، عملية الاتصال غير المباشرة بشعوب المجتمعات والدول الأخرى بغرض التأثير الإيجابي على الرأي العام فيه[1]. إذن فالدبلوماسية تعد جزءاً محورياً في تهيئة القبولالعام، الأمر الذي يؤدي إلى دعم سياساتها ووضعها[2]. وذلك كله بهدف واحد وهو إطلاع الدول الأخرى على أفضل ما لدى نظرائهم بما يعمل على تحسين صورة تلك الدولة لدى الجمهور، ومن ثم تعزيز التعاون والتفاهم المشترك.

ولقد طرأت على الدبلوماسية العامة تطورات كبيرة ومُتسارعة، خاصة مع ظهور الفضاء الإلكتروني، الأمر الذي نتج عنه ظهور ما يُسمى بـــ"الدبلوماسية الإلكترونية" Cyber Diplomacy. والتي شهدت تزايداً كبيراً في شعبيتها خلال الآونة الأخيرة. حيث أصبحت تميل الدول الغربية - على وجه التحديد – في استراتيجيتها الدبلوماسية إلى استخدام الإنترنت لنشر المعلومات الدبلوماسية عنها والتفاعل مع المواطنين (المستخدمين) وانتظار التغذية المرتدة Feed Back منهم. الأمر الذي يعمل على تقليل الوقت اللازم لرسم بعض السياسات الخارجية وسرعة وصول الجمهور إلى المعلومات الدبلوماسية[3].

كانت الولايات المتحدة أول دولة قامت بإطلاق وتبني مفهوم الدبلوماسية الإلكترونية أو الإلكترونية، نتيجة رغبتها في نشر الأفكار والسياسات الأمريكية في جميع أنحاء العالم، الأمر الذي استلزم اتباع استراتيجية توسيع مفهوم الدبلوماسية

1- شافي الدامر، دبلوماسية الـ Web 2.0، مجلة الإليكترونية الاقتصادية، العدد 5663، 13 أبريل 2009، مُتاح على: http://www.aleqt.com/2009/04/13/article_215424.html

2- فيليب تايلور، الدبلوماسية العامة ومكانتها في السياسة الخارجية، الدبلوماسي، العدد 52، أكتوبر 2010، ص: 39..

3- سارة يحيي Cyber Diplomacy: بعد غير تقليدي في العلاقات غير الرسمية بين الدول"، **مجلة اتجاهات الأحداث، ملحق مفاهيم المستقبل**، عدد 6 يناير 2015، تحرير إيهاب خليفة، صص 8-10.

العامة وتغيير النمط التقليدي له، فقامت بإنشاء مكتب EDiplomacy في عام 2003، تابع لوزارة الخارجية الأمريكية ومكتب إدارة موارد المعلومات، الذي تمثلت مُهمته الرئيسية في إمداد مُساعدة للدبلوماسيين الأمريكيين من خلال التواصل عبر الإنترنت، وجعل السياسة الخارجية للولايات المتحدة أكثر فاعلية[1].

وبعد ذلك وتحديداً في الفترة من 2006 حتى عام 2010، واصلت وزارة الخارجية الأمريكية العمل بقوة على تحقيق هدفها الاستراتيجي المُتمثِّل في توسيع مفهوم الدبلوماسية العامة وتعميم وتحفيز نشر الدبلوماسية الإلكترونية، فضلاً عن تحقيق مجموعة من الأهداف الفرعية المنبثقة عن ذلك الهدف الرئيسي والمتمثلة في: تقديم معلومات دقيقة، وخلق عملية ربط بين الدبلوماسيين وبعضهم البعض في أي مكان وفي أي وقت، وسهولة التنسيق مع الشركاء الخارجيين، وإدارة الأزمات بطريقة آمنة وفعَّالة، وخلق فريق من موظفي تكنولوجيا المعلومات على درجة عالية من التخصص لتحقيق مزيد من الابتكار في المجال[2]. وذلك في سبيل إعادة ترتيب أجندتها الدبلوماسية لمواجهة التحديات القديمة بطرق جديدة.

وتدريجياً قامت الولايات المتحدة الأمريكية بتبني مجموعة محددة من الفاعلين الذين لهم تأثيراتهم في المجال الدبلوماسي، بالإضافة إلى بعض الشركات، والشبكات العابرة للحدود الوطنية، وبعض المؤسسات، ومنظمات المجتمع المدني، والجماعات الدينية، والمواطنين أنفسهم لتنفيذ الاستراتيجية المتعلقة بالدبلوماسية الإلكترونية، وكانت النتيجة وجود ما يقرب من 230 صفحة عبر الفيسبوك متعلقة بالقضايا الدبلوماسية، و80 حساباً على تويتر، و55 قناة عبر اليوتيوب، و40 حساباً على فليكر.

1- المرجع السابق.

2-Tang Xiaosong& Lu Yanfang, New Developments in the E-diplomacy of Western Countries and Their Implications for China, Op. Cit.,, p p: 145 - 146.

هذا فضلاً عن تنفيذ بعض البرامج والمبادرات الخاصة بتطبيق الدبلوماسية الإلكترونية مثل[1]:

- **الحوارات الديمقراطية (Democracy Dialogues):** وهو موقع تفاعلي متعدد اللغات، تم إنشاؤه في عام 2006 من قِبَل وزارة الخارجية الأمريكية. ويُعد منصة لتشجيع النقاش حول المبادئ الديمقراطية المشتركة، وكل شهرين يتم طرح موضوع ديمقراطي جديد للمُناقشة.

- **فريق التواصل الرقمي (Digital Outreach Team):** وهو عبارة عن مجموعة أفراد تابعين لوزارة الخارجية الأمريكية تقوم بالتواصل من خلال الحوارات والمناقشات السياسية الموجودة على شبكة الإنترنت باللغات العربية والصومالية والأردية. وقد تم إنشاء هذا الفريق في نوفمبر عام 2006 ليتكفل بمهمة طرح وشرح سياسات الولايات المتحدة الخارجية، بالإضافة إلى شرح وتقديم الجوانب الاجتماعية والثقافية للمجتمع الأمريكي بطريقة يسهل فهمها.

- **ديب نوت (Dipnote):** والذي ظهر في عام 2007، حيث صممته وزارة الخارجية الأمريكية بهدف فتح منبر للجماهير الأجنبية لإشراكهم في سياستها من خلال المدونات. وكذلك التشجيع على إجراء حوارات مفتوحة بكل ما يتعلق بالولايات المتحدة الأمريكية والدبلوماسية العامة. ويُعد قبول كافة ردود الأفعال، سواء السلبية أو الإيجابية، جزءاًرئيسياً من فلسفة الموقع، لأنه يُعد مجساً حقيقياً لنبض الجماهير الأجنبية. وبعد ذلك تمت إضافة مجموعة من التعديلات عليه في عام 2009، وتوسعت أنشطته لتتضمن: إعلام الجماهير عن السفر، والخطب، المجهودات التي تقوم بها وزيرة الخارجية الأمريكية هيلاري كلينتون، وموظفو وزارة الخارجية والدبلوماسيون حول العالم، وترجمة خطابات الرئيس الأمريكي إلى لغات مختلفة. والهدف من كل ذلك هو جعل الدبلوماسية العامة الأمريكية في متناول الجميع الذين لا يتحدثون اللغة الإنجليزية وأولئك الذين يستخدمون الإنترنت.

1- سارة يحيي، مرجع سبق ذكره.

- فضاء الرأي (Opinion Space): قامت وزارة الخارجية الأمريكية وجامعة كاليفورنيا (مركز بيركلي للإعلام الجديد) بإنشاء هذا الموقع في فبراير 2011. ويقوم الموقع بإتاحة التعبير عن وجهات النظر بشأن العديد من الموضوعات من السياسة وحتى الاقتصاد. وعندما تقوم الجماهير بتسجيل وجهة نظرهم يتم إبلاغهم بموقفهم من القضية التي عبَّروا عن آرائهم فيها وتعريفهم بالمُشاركين المتفقين معهم. ومن خلال طريقة تصميم الموقع الذي يعتمد على الألعاب في الاقتراع واستطلاعات الرأي يُشجع الأشخاص من جميع أنحاء العالم على المُشاركة في المناقشات وتقييم استجابات الآخرين.

- **المجتمع المدني 2.0 (Civil Society 2.0):** يعمل الموقع على ربط مجتمع تكنولوجيا المعلومات والاتصالات مع منظمات المجتمع المدني على مستوى العالم، وكذا توفير أحدث التكنولوجيا لمنظمات المجتمع المدني، والهدف منه هو تدعيم جهود المجتمع المدني في جميع أنحاء العالم لكونه يُساعد على جعل المجتمعات أكثر رخاء واستقراراً. وللموقع أدواته المتمثلة في: الرسائل النصية، والمواقع، ومواقع التواصل الاجتماعي لربط المشتركين ببعضهم البعض. وتقوم وزارة الخارجية بإرسال مجموعة من التكنولوجيين إلى مناطق بعينها لتعليم السكان المحليين كيفية استخدام التكنولوجيا، وتعليمهم كيفية بناء موقع على شبكة الإنترنت، وكيفية التدوين، وكيفية إطلاق حملة الرسائل النصية، وبناء مجتمع دولي على الإنترنت، وطرق الاستفادة من الشبكات الاجتماعية من أجل قضية ما، الأمر الذي يؤدي إلى إقامة مجتمع تكنولوجي.

كما أطلقت الولايات المتحدة في أواخر 2011 موقعاً إلكترونياً اعتبرته بمنزلة سفارة افتراضية للولايات المتحدة في إيران، تقدم من خلاله للإيرانيين معلومات عن تأشيرات الدخول وبرامج التبادل الطلابية على الرغم من عدم وجود علاقات دبلوماسية رسمية بين البلدين[1]، فيما يمكن تسميته بالدبلوماسية الإلكترونية، وبمجرد تدشين الموقع الإلكتروني قامت السلطات الإيرانية بحجبه، الأمر الذي ندد به البيت الأبيض وقال المتحدث باسم البيت الأبيض جاي كارني: "ندين الجهود التي تبذلها الحكومة الايرانية لمنع الشعب من حرية الوصول إلى السفارة الافتراضية"[2].

1- واشنطن تطلق سفارة افتراضية لدى طهران على الإنترنت، **موقع اليوم السابع**، 26 ديسمبر 2011، بتاريخ مطالعة 27 أبريل 2014، للمزيد يمكن المطالعة على:
http://www1.youm7.com/News.asp?NewsID=548853&SecID=286&IssueID=0#.U1wTP4GSwoI
2- واشنطن تندد بحجب طهران " سفارتها الافتراضية" على الإنترنت، **موقع BBC**،5 ديسمبر 2011، بتاريخ دخول 18 أبريل 2014، يمكن المطالعة على:
http://www.bbc.co.uk/arabic/worldnews/2011/12/111207_iran_us_embassy_virtual_internet.shtml

5- مواجهة فكر الحركات الإرهابية:

تعمل الولايات المتحدة الأمريكية على مكافحة وجود الحركات الإرهابية على شبكة الإنترنت، حيث تعمل هذه الحركات على استقطاب الأفراد وإقناعهم بالأفكار المتطرفة، كما أنها تستخدم الإنترنت في عمليات التواصل والتخطيط لهجمات إرهابية، مما دفع الولايات المتحدة إلى مكافحة وجودهم على شبكة الإنترنت، من خلال تعقب المواقع التي تبث فكراً متطرفاً، ومحاولة اختراق البريد الإلكتروني والحسابات الإلكترونية للشخصيات التي تتبنى هذا الفكر، وقد كشفت إحدى الوثائق السياسية التي سربها سنودن عن قيام وكالة الأمن القومي الأمريكي NSA بالتجسس إلكترونياً على إسلاميين متشددين يدخلون باستمرار إلى مواقع إلكترونية إباحية، ومن بين الأدلة التي جمعتها الوكالة مشاهد تظهر متشدداً إسلامياً وهو يشاهد محتوى إباحياً فاضحاً على الإنترنت، أو يستخدم كلاماً جنسياً فاضحاً مع فتيات، وذلك بهدف كشف نفاقهم، حيث إنهم يدعون في العلن إلى الجهاد والالتزام الديني[1].

وكانت السلطات الأميركية قد شنت عملية سرية لدس رسائل بريد إلكتروني مزيفة ورسائل على بعض المواقع بغرض مواجهة جهود الارهابيين الرامية الى التخطيط لشن هجمات وجمع تبرعات وتجنيد أعضاء جدد عبر الشبكة[2].

1- الاستخبارات الأمريكية تجسست على إسلاميين متشددين يدخلون مواقع إباحية، **موقع فرنسا 24**، بتاريخ 28 نوفمبر 2013، بتاريخ دخول 21 أبريل 2014، يمكن المطالعة على:

http://www.france24.com/ar/20131128-%D8%A5%D8%AF%D9%88%D8%A7%D8%B1%D8%AF-%D8%B3%D9%86%D9%88%D8%AF%D9%86-%D8%AA%D8%AC%D8%B3%D8%B3-%D8%A7%D9%84%D9%88%D9%84%D8%A7%D9%8A%D8%A7%D8%AA-%D8%A7%D9%84%D9%85%D8%AA%D8%AD%D8%AF%D8%A9-%D8%A5%D8%B3%D9%84%D8%A7%D9%85%D9%8A%D9%88%D9%86-%D8%AC%D9%86%D8%B3-%D8%A5%D8%A8%D8%A7%D8%AD%D9%8A%D8%A9/

2- ايريك شميت وتوم شانكر، واشنطن تكافح الإرهاب العالمي بأسلوب الحرب الباردة، **موقع الشرق الأوسط**، 20 مارس 2008، تاريخ دخول 21 أبريل 2014، يمكن المطالعة على:

http://classic.aawsat.com/details.asp?section=4&article=463429&issueno=10705#.U1TbyFWSwoI

الخلاصة:

استطاعت الولايات المتحدة من خلال توظيف قوتها الإلكترونية تغيير بعض المفاهيم الاستراتيجية، خاصة فيما يتعلق بالتهديدات غير التقليدية للأمن، فغيرت من مفاهيم التجسس، وانتقلت من مرحلة التجسس على الأفراد إلى التجسس على الشعوب، واستطاعت تحقيق "الآنية" في التجسس على زعماء وقادة العالم، فتمكنت من سماع وتسجيل مكالماتهم الهاتفية في وقتها الحقيقي، مما دفع هؤلاء القادة إلى التفكير في إنشاء شبكات إنترنت إقليمية لا تعتمد على الشركات أو الخوادم الأمريكية، حتى تحتفظ ببياناتها سرية، وأدرك حلفاء الولايات المتحدة مثل فرنسا وألمانيا أنهم أيضاً موضع اختراق من الولايات المتحدة.

ونجحت في التواصل مع الشعوب من خلال بث رسائل سياسية عبر مواقع التواصل الاجتماعي تدعم الرؤية الأمريكية للقضايا المثارة على الساحة المجتمعية، واعتمدت على القوة الإلكترونية في تشويه بعض الرموز الجهادية وكشف فضائحهم الجنسية من خلال اختراق حساباتهم البريدية، وتمكنت من إدخال مفهوم جديد في الدبلوماسية، وهو الدبلوماسية الإلكترونية، من خلال تدشينها سفارة افتراضية مع إيران، وعلى الرغم من عدم استمرار التجربة، إلا أنها حققت السبق في هذا المجال.

المبحث الثاني

استخدام القوة الإلكترونية الأمريكية في التفاعلات الدولية العسكرية

تقوم الولايات المتحدة باستخدام قوتها الإلكترونية لتحقيق بعض الأهداف العسكرية، سواء من خلال تحقيق الردع الإلكتروني من خلال تعظيم معايير الأمان لشبكة الإنترنت الداخلية وسرعة كشف أماكن الاختراق والتعرف على مصادرها والتعامل الفوري معها، أو من خلال الهجمات الإلكترونية الخارجية التي تشنها لتحقيق أهداف عسكرية.

وعلى الرغم من أن هذا النوع من التهديدات لم يرتق بعد ليتساوى مع التهديدات العسكرية التقليدية في حسم المعارك الحربية.

فإن ميزتها النسبية تكمن في ربط الوحدات العسكرية بعضها ببعض بالأنظمة العسكرية الإلكترونية، بما يسمح بسهولة تبادل المعلومات وتدفقها، وسرعة إعطاء الأوامر العسكرية، والقدرة على إصابة الأهداف وتدميرها عن بعد. وقد تتحول هذه الميزة إلى نقطة ضعف، إن لم تكن الشبكة الإلكترونية المستخدمة في ذلك مؤمنة جيداً من أي اختراق خارجي، منعاً للتجسس أو التلاعب بالبيانات أو تدميرها أو التلاعب بالأنظمة العسكرية وإعادة توجيه أسلحة الخصم ضد أهداف وهمية أو صديقة.

مثلت القوة الإلكترونية أحد الأسلحة العسكرية التي يمكن أن تحقق بها الولايات المتحدة الأمريكية أهدافها بفاعلية، سواء من خلال سرقة المعلومات العسكرية والتلاعب بها، أو استهداف البنى التحتية العسكرية وشبكات الاتصال اللاسلكية للخصوم، أو ممارسة نوع من الحروب النفسية عبر الانترنت، أو بتطوير الاستراتيجية العسكرية لحلف الناتو لكي تشمل الفضاء الإلكتروني.

وفيما يلي بعض النماذج التطبيقية لاستخدام القوة الإلكترونية في إدارة التفاعلات العسكرية الأمريكية:

1- سرقة المعلومات والبيانات العسكرية أو التلاعب بها:

انطلقت في عام 2008 واحدة من أخطر الهجمات ضد أنظمة حواسب الجيش الأمريكي، من خلال وصلة USB بسيطة متصلة بكمبيوتر محمول تابع للجيش في قاعدة عسكرية موجودة في الشرق الأوسط، ولم يتم اكتشاف انتشار برامج التجسس في كل من الأنظمة السرية وغير السرية في الوقت المناسب، مما شكل ما يشبه جسراً رقمياً، تم من خلاله نقل آلاف الملفات من البيانات إلى خوادم خارجية Servers، كما تم استهداف أكثر من 72 شركة من بينها 22 مكتباً حكومياً و13 من مقاولي قوات الدفاع بهدف سرقة معلومات حول الخطط والمباني العسكرية[1].

وفي تقرير مقدم إلى الكونجرس الأمريكي تم تسريب أجزاء منه إلى صحيفة الواشنطن بوست نشرت معلومات عن قيام قراصنة صينيين يعملون لصالح الحكومة الصينية بسرقة معلومات عسكرية أمريكية حول منظومات مضادة للصواريخ من طراز "باتريوت ب أ س-3" ونظام "ثاد"، بالإضافة إلى المعلومات حول الطائرات والسفن العسكرية، مما مكن الحكومة الصينية من استخدام هذه المعلومات لتطوير تقنياتها العسكرية، وهو ما وفر عليها الكثير من الوقت والجهد والأموال لتطوير هذه الأسلحة[2].

1- د. أولاف تايلر، التهديدات الجديدة: الأبعاد الإلكترونية، **موقع مجلة حلف الناتو**، 11 سبتمبر 2011، بتاريخ دخول 16 أبريل 2014، يمكن المطالعة على الرابط التالي:

http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/AR/index.htm

2- Ellen Nakashima, Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies, **The Washington Post,March 27th, 2013,** AccessedOn April 17th, 2014. http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weaponsConfidential report lists U.S. weapons system designs compromised by Chinese cyberspies-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html?hpid=z1

وتقوم العقيدة الصينية على اعتقاد أساسي مفاده ... ضرورة قيام جمهورية الصين الشعبية باستخدام القوة الإلكترونية – إلى جانب أدوات أخرى - بهدف إعاقة أجهزة الاستطلاع الإلكترونية والأقمار الصناعية الأمريكية، لتعطيل قدرات الولايات المتحدة الأمريكية على التدخل في أي صراع في منطقة شرق آسيا والمحيط الهادي[1]، وعادة ما تستخدم الصين قدراتها الإلكترونية لتحقيق أهداف خاصة بجمع معلومات اقتصادية أو القيام بعمليات استخباراتية عسكرية، أو القيام بعمليات تجسس على المواطنين والتحكم في تدفق البيانات عبر شبكات الإنترنت، فضلاً عن مراقبة أنشطة بعض الحكومات الأجنبية من خلال القيام بعمليات قرصنة إلكترونية على قواعد بياناتها.

أنشأت الصين محطتين للتجسس على الشبكات في دولة لا تبعد كثيراً عن الولايات المتحدة هي كوبا بإذن من حكومة كاسترو، حيث أقام الجيش الصيني منشأة لرصد التحركات الأمريكية على الإنترنت، ومحطة أخرى لمراقبة اتصالات وزارة الدفاع الأمريكي، وفي الوقت الذي أعلنت فيه الصين عن إنشاء وحدات حرب الفضاء الإلكتروني عام 2003 تعرضت الولايات المحتدة لواحدة من أسوأ حلقات التجسس الإلكتروني ويطلق عليها اسم Titan Rain أي مطر العمالقة[2]، وفيها تم سحب ما يتراوح بين 10 - 20 تيرابايت من المعلومات من شبكة البنتاجون غير السرية، واعتمدت الهجمة على تحديد مواطن الضعف بطريقة منهجية في شبكة البنتاجون والشبكات الأخرى المستهدفة ثم استغلالها لانتزاع المعلومات من خلال أجهزة خادمة تقع في كوريا الجنوبية وهونج كونج، كما تمكن المحققون من تتبع حركة التدفق من هذه الأجهزة الخادمة الوسيطة إلى الجهاز الخادم النهائي ومقره جواندونج في الصين[3].

كما قام قراصنة الكترونيون صينيون بشن بضع هجمات على مواقع شركة "لوكهيد مارتين" الإلكترونية الأمريكية، حيث سرقوا معلومات عن تكنولوجيا

1- Larry Wortzel, **Defense dossier**, American Foreign Policy Council, August 2012, p1.
2- James A.Lewis,**ComputerEspionage,Titan Rain and China,** CSIS, ON May 4, 2014**http://csis.org/files/media/csis/pubs/051214_china_titan_rain.pdf**
3- ريتشارد كلارك وروبرت نيك، **مرجع سبق ذكره،** ص ص 69-71.

تصنيع مقاتلة "إف – 35" التي استخدمتها الصين فيما بعد لدى تصميم وتصنيع مقاتلة "تي 20" الصيني. وقد أطلقت المخابرات الأمريكية على سلسلة من الهجمات التي شنها القراصنة الصينيون عام 2007 تسمية "الجحيم البيزنطي".

وكانت الهجمات الإلكترونية تستهدف المؤسسات الصناعية الحكومية الأمريكية[1]، ووفقاً لبيان إحدى الشركات الأمريكية العاملة بمجال مراقبة الهجمات الإلكترونية، أشار إلى أن الشركة رصدت خلال عامي 2011-2012 عدداً كبيراً من الهجمات الإلكترونية مصدرها شنغهاي الصينية، شملت مقاولين لدى وزارة الدفاع الأمريكية يعملون على صناعة وتطوير الطائرات بدون طيار Drones الأمريكية، بهدف سرقة معلومات حول هذه الطائرات وكيفية صناعتها وتطويرها[2].

كما نشرت صحيفة الجارديان تقريراً في ديسمبر 2009 أشارت فيه إلى قيام السلطات في كوريا الجنوبية بالتحقيق في واقعة قرصنة إلكترونية تم اتهام كوريا الشمالية فيها بسرقة خطط كورية أمريكية مشتركة تتعلق بتحركات في حالة وجود حرب في شبه الجزيرة الكورية من حيث إمكان نشر القوات والأهداف العسكرية المقصودة، وكيفية التأسيس لاحتلال كوريا الشمالية بعد الحرب post - War Occupation، وقد أرجعت التحقيقات أن عملية الاختراق قد حدثت حينما قام ضابط بالقوات الكورية الجنوبية باستخدام كارت ذاكرة خارجي USB memory غير مؤمن متصل بشبكة الإنترنت[3].

كما تم اختراق معمل الفيزياء المتطورة بجامعة جونز هوبكنز الذي يجري بحوثاً لصالح الحكومة الأمريكية تقدر قيمتها بمئات الملايين من الدولارات من تقنيات

1- أمريكا تتهم الصين بسرقة تكنولوجيا صنع مقاتلة "إف – 35"، **موقع روسيا اليوم**، تاريخ 14 مارس 2014، بتاريخ مطالعة 20 أكتوبر 2014، يمكن المطالعة على:
http://arabic.rt.com/news/668023/

2- Hacking U.S. Secrets, China Pushes for Drones, **The New York Times**, Sep 21, 2013, Accessed on April 17th, 2014, http://www.nytimes.com/2013/09/21/world/asia/hacking-us-secrets-china-pushes-for-drones.html?pagewanted=all&_r=2&

3-North Korean hackers may have stolen US war plans, **The Guardian**, December 18, 2009,, Accessed On April 18th, 2014,
http://www.theguardian.com/world/2009/dec/18/north-south-korea-hackers

الفضاء الخارجي إلى الأدوية الحيوية والمشروعات السرية المتعلقة بالأمن القومي، حيث تمكن قراصنة في عام 2009 من اختراق المعمل المعروف بتأمين الشبكات الخاصة به، ولم يتمكن القائمون على حماية الشبكة من وقف عملية القرصنة وسرقة المعلومات إلا من خلال عزل المعمل عن الإنترنت وفصل الشبكة عنه[1].

وفي شهر يونيو 2007 تعرض حساب البريد الإلكتروني المعلن لوزير الدفاع الأمريكي للاختراق من قبل متسللين أجانب مجهولين، كجزء من سلسلة هجمات أكبر للوصول إلى الشبكات التابعة للبنتاجون واستغلالها[2].

في يوليو 2011 كشف فيه عن الاستراتيجية الإلكترونية لوزارة الدفاع، ذكر نائب وزير الدفاع الأمريكي أن إحدى الجهات المتعاقدة مع وزارة الدفاع قد تعرضت للاختراق وتمت سرقة 24000 ملف من وزارة الدفاع[3].

1- ريتشارد كلارك وروبرت نيك، **مرجع سبق ذكره**، ص 156.
2- **تاريخ الهجمات الإلكترونية،مجلة حلف الناتو**، تاريخ مطالعة 18 أبريل 2014، يمكن المطالعة على:
http://www.nato.int/docu/review/2013/Cyber/timeline/AR/index.htm
3- المرجع السابق.

2- استهداف البنى التحتية المدنية Cyber Infrastructure:

حذَّر المستشار السابق للبيت الأبيض ريتشارد كلارك، من أنّ الولايات المتحدة قد تتعرض لهجوم إلكتروني، قد يدمرها في غضون 15 دقيقة، لأنها لم تستعد بعد لمثل هذا الهجوم؛ خلافاً لدول أخرى مثل الصين وروسيا وحتى كوريا الشمالية، حيث أوضح أن خدمة الإنترنت حينما تتعرض للتشويش، فإنّ احتمالات كارثية يمكن أن تحصل، مثل اندلاع النيران وانفجارات بمصاف في فيلادلفيا وهيوستن، وتعطل المصانع الكيماوية وانتشار غيوم من غاز الكلور القاتل في الجو، كما سيكشف مراقبو حركة الطيران عن عمليات اصطدام للطائرات في الجو، وتحطم قطارات الأنفاق في نيويورك وواشنطن ولوس أنجلوس، وسيعم الظلام في أكثر من 150 مدينة أمريكية، ويقضي أكثر من عشرات الآلاف من الأمريكيين في هجوم لا يختلف عن الهجوم النووي، وكل ذلك يمكن أن يحصل خلال 15 دقيقة فقط، وعلى يد شخص واحد فقط[1].

ومن ناحيتها أعدت مجموعة حرب المعلومات بكلية جيش الولايات المتحدة الحربية The Information in Warfare Group of the U.S. Army War College تقريراً حول القوة الإلكترونية للصين والأمن القومي الأمريكي، تمت الإشارة فيه إلى أن استخدام القوة الإلكترونية وتوظيف شبكات الإنترنت أصبح مصدر تهديد، خاصة ضد الولايات المتحدة الأمريكية، وذلك لسهولة استخدامها ورخص تكلفتها، وهو ما قد يدفع أعداء الولايات إلى استخدامها ليس فقط في المجال العسكري، ولكن أيضاً في المجالين الاقتصادي والسياسي[2].

وقد خلص التقرير إلى أنه منذ 1991 تسعى جمهورية الصين الشعبية لتمويل وتطوير والحصول على تكنولوجيا إلكترونية متطورة في المؤسسات الحكومية والعسكرية والمدنية، وذلك لبناء قوة سياسية واقتصادية صينية في مواجهة الولايات

1- **هجوم إلكتروني يهدد بتدمير أمريكا في 15 دقيقة**، 9 مايو 2010، بتاريخ دخول 18 أبريل 2014، يمكن المطالعة على: http://www.hespress.com/international/20914.html

2- Colonel Jayson M. Spade Edited By, Jeffrey L. Caton, **China's Cyber Powerand America's National Security,** (U.S. Army War College, May 2012) P1.

المتحدة الأمريكية، حيث أشار التقرير إلى أن جيش التحرير الشعبي الصيني يعد نفسه إلى حرب إلكترونية شاملة، وذلك من خلال استخدام الإنترنت في جمع المعلومات والسيطرة على أجهزة الاتصالات والمعلومات، وتدمير البنية التحتية، وإصابة الاقتصاد القومي بأضرار جسيمة، كتمهيد لخوض صراع مسلح، وتوظيف الإنترنت أيضاً في الحروب النفسية ضد إرادة الشعب الأمريكي، وقد تعرض التقرير لاستخدام الصين للقوة الإلكترونية ضد بعض الدول مثل تايوان في 2005 وألمانيا في 2007، كما قامت بتنفيذ هجمات إلكترونية على أكثر من 1200 جهاز كمبيوتر في 103 دول عام 2009.

وفي الفترة من 30 أبريل حتى 7 مايو 2001، تعرض ما يقرب من 1200 موقع أمريكي لهجمات من قراصنة صينيين، شملت مواقع البيت الأبيض، والقوات الجوية الأمريكية، ووزارة الطاقة الأمريكية[1]، وذلك على خلفية اصطدام مقاتلة صينية من طراز "J-8 land" مع طائرة تجسس أمريكية من طراز "EP-3E" فوق جزيرة "هاينان" الصينية في الأول من أبريل 2001، والذي نتج عنه تحطم الطائرة الصينية وغرقها وفقدان طيارها وهبوط الطائرة الأمريكية اضطرارياً في مطار جزيرة "هاينان" الصينية وسلامة طاقمها المكون من 24 فرداً. وقد تسببت هذه الحادثة في نشوب أزمة سياسية بين البلدين مرت بكثير من المحطات والمنعطفات الحرجة قبل أن يتنازل كل طرف عن جزء من حقوقه التي يرى على ضوئها أن موقفه هو الصواب وما دونه هو الخطأ[2].

وفي عام 2003 نجح برنامج يسمى Slammer Worm – لم يتضح مصدره – في الدخول إلى شبكة الكهرباء وإبطائها، كما ساهم عيب في أحد البرامج المستخدمة في نظام SCADA في إبطاء شبكة الكهرباء، وعندما تسبب سقوط إحدى الأشجار في ارتفاع الحمل الكهربائي في أحد خطوط الكهرباء في أوهايو الأمريكية، لم تستجب

1-Michael Vatis, **Cyber Attacks During the War on Terrorism: A Predictive Analysis**, Institute For Security Technology StudiesAt Dartmouth College, September 2001, On http://www.ists.dartmouth.edu/docs/cyber_a1.pdf
2-Ibid.

الأجهزة التي كان من المفترض أن تعمل على إيقاف الأثر التتابعي للحادث، حتى وصل انقطاع التيار إلى جنوب ولاية نيوجيرسي، ونتيجة لذلك باتت ثماني ولايات أمريكية ومقاطعتان كنديتان و50 مليون شخص بلا كهرباء، وبلا أي شيء يحتاج للكهرباء لتشغيله، مثل أنظمة المياه في كليفلاند[1]، كما نشرت صحيفة وول ستريت جورنال تقريراً في عام 2009 أشارت فيه إلى تورط الصين وروسيا في اختراق شبكة الكهرباء القومية الأمريكية، وعلى الرغم من أن عملية الاختراق لم تشمل مهاجمة الشبكة، فإنها ساعدت في استطلاع الشبكة والتجسس عليها وتصفح نظام تشغيلها، مما قد يساعد في شن هجمات إلكترونية مستقبلية على شبكة الكهرباء الأمريكية والتسبب في خسائر فادحة في حالة وقوع حرب إلكترونية بينهما وبين الولايات المتحدة[2].

1- ريتشارد كلارك وروبرت نيك، **مرجع سبق ذكره**، ص ص 172- 128.

2- Electricity Grid in U.S. Penetrated By Spies, **The wall streetJournal**, April 8, 2009, Accessed On 11 July 2014, on http://online.wsj.com/news/articles/SB123914805204099085

3- تدمير البنى التحتية الإلكترونية العسكرية:

لم يقتصر الأمر على تهديد البنى التحتية المدنية، بل شمل أيضاً البنى التحتية العسكرية، حيث حقق فيروس ستاكسنت الذي ظهر في عام 2010 قفزة نوعية وكمية في القدرات المدمرة للحرب الإلكترونية، حيث أعلنت الاستخبارات الإيرانية أن فيروس ستاكسنت أصاب ما يقدر بستة عشر ألف جهاز كمبيوتر، وذلك بعد أن تعرضت لهجوم في أكتوبر 2010، وآخر في أبريل 2011[1]، وتسبب في تعطيل حوالي 1000 من أجهزة الطرد المركزي في ناتانز، فضلاً عن تعطيل إيران لمدة سنتين عن تخصيب اليورانيوم[2]، وقد تبنت إسرائيل المسؤولية عن شن هجمات ستاكسنت بالتعاون مع الولايات المتحدة للعمل على تعطيل المنشآت النووية كجزء من منصة لإطلاق الفيروسات الخطرة تم تطويرها عام 2007 وتمت تجربتها في إسرائيل.

1-Iran says Stuxnet virus infected 16,000 computers,**Foxnews**, Feb 18, 2012, Accessed On April 17th, 2014 http://www.foxnews.com/world/2012/02/18/iran-says-stuxnet-virus-infected-16000-computers/

2- باربرا سلافين، وجيسون هيلي، **الحرب الافتراضية: هل تملك طهران القدرة على مهاجمة واشنطن الكترونيا؟**، تقرير منشور على موقع المركز الإقليمي للدراسات السياسية والاستراتيجية، بتاريخ دخول 14 أبريل 2014، يمكن المطالعة على:

http://rcssmideast.org/%D8%A7%D9%84%D8%AA%D8%AD%D9%84%D9%8A%D9%84%D8%A7%D8%AA/%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%A3%D9%82%D9%84%D9%8A%D9%85%D9%89/%D8%A7%D9%84%D8%AD%D8%B1%D8%A8-%D8%A7%D9%84%D8%A7%D9%81%D8%AA%D8%B1%D8%A7%D8%B6%D9%8A%D8%A9.html

4- السيطرة على الأنظمة العسكرية:

لا يقتصر الاستخدام العسكري للفضاء الإلكتروني فقط على ما يوفره من معلومات حول صناعة وتطوير الأسلحة، ولا يقتصر أيضاً على ما يمكن سرقته من معلومات واستراتيجيات عسكرية خاصة بالخصم أو التلاعب بها أو حتى محوها، بل إن الأمر أعقد من ذلك بكثير، فالمؤسسات الاستراتيجية والعسكرية متصلة بأنظمة إلكترونية، ونظم الدفاع الجوي والطيران وتوجيه الأسلحة، مرتبطة أيضاً بأنظمة إلكترونية، وإدارة الأقمار الصناعية والغواصات النووية والصناعات الحربية، تتم أيضاً من خلال هذه الأنظمة، وإذا كان الفرد العادي يستخدم نظام الملاحة GPS لتحديد موقعه وموقع الآخرين، فإن النسخة العسكرية من هذا النظام تستخدم أيضاً في توجيه الطائرات والبوارج الحربية.

وتكمن الخطورة المحتملة في إمكانية السيطرة على هذه النظم الإلكترونية من خلال هجمات قراصنة محترفين أو جيوش نظامية إلكترونية، وإخراجها عن سيطرة القيادة العليا للدولة، حيث يمكن اختراق أنظمة توجيه الصواريخ وتوجيهها نحو أهداف صديقة، أو السيطرة على الطائرات بدون طيار، أو الغواصات النووية في أعماق البحار، أو السيطرة على الأقمار الصناعية العسكرية في الفضاء الخارجي وإخراجها من سيطرة الخصم عليها، فاللوجستيات والقيادة والتحكم ووضع الأساطيل البحرية وكل شيء حتى تحديد الأهداف وإصابتها يعتمد على برامج الحاسوب وغيرها من التقنيات المتعلقة بالفضاء الإلكتروني.

حيث نجحت قوات الدفاع الجوي الإيرانية في السيطرة إلكترونياً على طائرة من دون طيار أمريكية من طراز "RQ-170"، في ديسمبر 2011 وإرغامها على النزول في حالة شبه سليمة[1]، وذلك من خلال اختراق إلكتروني للطائرة من دون التسبب في تدميرها من خلال إطلاق النار، وقد أكد الجنرال أمير علي حجي زادة، قائد القوات

1- ايران تسقط طائرة استطلاع أمريكية بدون طيار، **وكالة رويترز للأنباء**، تاريخ 17 ديسمبر 2011، تاريخ مطالعة 17 أبريل 2014،على الرابط التالي:

http://arabic.rt.com/news/573311/

الجوية والفضائية في الحرس الثوري الإيراني، في أبريل 2012، أن طهران نجحت في اختراق أسرار طائرة الاستطلاع من دون طيار الأميركية[1]، مما يفتح المجال واسعاً أمام إمكانية السيطرة عن بعد على جيش من هذه طائرات العدو التي تعمل بدون طيار وتوجيهها إلى أهدافه المرجوة، ولم يستبعد المركز الصحفي في البنتاجون الأمريكي لاحقاً أن تكون الطائرة المذكورة ذات الطائرة التي تم الإعلان عن فقدان الاتصال بها قبل أسبوع من اسقاطها بعد مهمة في غرب أفغانستان[2].

في سبتمبر 2007، استطاعت قوات الجو الإسرائيلي تدمير مبنى على الأراضي السورية، حيث كشفت وسائل الإعلام الأمريكية أن هذا المبنى كان سيستخدم لتصنيع أسلحة نووية بمساعدة من كوريا الشمالية، وأن القوات الإسرائيلية بمساعدة أمريكية، وغض طرف تركي عن تشكيلات قوات الجو الإسرائيلي، استطاعت أن تخترق المجال الجوي السوري من ناحية تركيا، وأن تقوم بتدمير هذا المبنى من دون أن تلتقط إشارات الرادارات الخاصة بالدفاع الجوي السوري دخول أي طائرات عسكرية، حيث نجحت إسرائيل في السيطرة على شبكة الدفاع الجوي الروسية التي تمتلكها سوريا، وذلك قبل الغارة الجوية بساعات، وأظهرت صوراً غير حقيقية على شاشات الرادار، كانت خالية من أي شيء، في الوقت الذي قامت فيه طائرات من طراز "إيجل" و"فالكون" بتدمير المبنى وتحويله إلى ركام، ولم يكن بالمستطاع إطلاق صواريخ الدفاع الجوي السوري نظراً لعدم وجود أهداف يحددها لها نظام المراقبة كي تتجه إليه، ولو لم تنجح إسرائيل في السيطرة على شبكة الدفاع الجوي الصوري لاستطاعت القوات السورية اسقاط هذه الطائرات، فهي مصنوعة

1- ايران تؤكد اختراق اسرار الطائرة الاميركية آر كيو- 170، **موقع إيلاف**، بتاريخ 24 أبريل 2012، بتاريخ دخول، 17 أبريل 2014، يمكن المطالعة على:

http://www.elaph.com/Web/news/2012/4/731015.html#sthash.eQfwfoLU.dpuf

2- البنتاجون لا يعلق على خبر اسقاط ايران طائرة امريكية بلا طيار، **وكالة رويترز للأنباء**، بتاريخ مطالعة 23 أكتوبر 2014، يمكن المطالعة على:

http://arabic.rt.com/news/573311-%D8%A7%D9%8A%D8%B1%D8%A7%D9%86_%D8%AA%D8%B3%D9%82%D8%B7_%D8%B7%D8%A7%D8%A6%D8%B1%D8%A9_%D8%A7%D8%B3%D8%AA%D8%B7%D9%84%D8%A7%D8%B9_%D8%A7%D9%85%D8%B1%D9%8A%D9%83%D9%8A%D8%A9_%D8%A8%D8%AF%D9%88%D9%86_%D8%B7%D9%8A%D8%A7%D8%B1

من الصلب والتيتانيوم، وشكلها يتميز بحواف وأركان حادة، وقذائفها تتدلى من أجنحتها، مما يعني ضرورة التماعها بكل وضوح على شاشات الرادار السورية[1].

وعلى الرغم من قلة الوقائع الفعلية التي تدعم هذا النمط خلال فترة الدراسة، أو وجود تسريبات عسكرية عن نجاح إحدى الدول في السيطرة على أنظمة عسكرية إلكترونية عن بعد، فإن التطورات التكنولوجية المتسارعة، تجعل إمكانية حدوثه أمراً بات بالقريب، وهنا يتحول الاستخدام العسكري للقوة الإلكترونية من مجرد إصابة البعد المعلوماتي إلى إصابة البعد المادي والبشري وتدميره كلياً، وهو ما يتوقف على قدرة الخصم في تعزيز قدراته الدفاعية وتأمين شبكاته وأنظمته الإلكترونية.

1- ريتشارد كلارك وروبرت نيك، **حرب الفضاء الإلكتروني .. التهديد التالي للأمن القومي وكيفية التعامل معه**، دراسات مترجمة 52، (أبوظبي، مركز الإمارات للدراسات والبحوث الاستراتيجية، 2014)، ص ص 16 -20.

5- توظيف الأحلاف العسكرية:

كان لهجمات الحادي عشر من سبتمبر أثر مهم في تغيير استراتيجية الولايات المتحدة العسكرية، ليس على المستوى الداخلي فحسب، بل أيضاً على مستوى الأحلاف العسكرية، وفيما يتعلق بالقوة الإلكترونية فبعد عام واحد من الهجمات، أطلقت منظمة حلف شمال الأطلنطي (الناتو) بقيادة الولايات المتحدة الأمريكية دعوة لتحسين قدراته الدفاعية ضد الهجمات الإلكترونية، وركز الحلف في السنوات التالية بشكل أساسي على تنفيذ تدابير الحماية السلمية المطلوبة للجانب العسكري، حيث شجعت الهجمات الإلكترونية التي وقعت في إستونيا في عام 2007 التحالف لإعادة التفكير في احتياجه إلى سياسة دفاع إلكتروني ودفع التدابير المضادة للهجمات إلى مستوى جديد.

ومن ثم وضع التحالف للمرة الأولى في تاريخه سياسة رسمية "للدفاع الإلكتروني" تم اعتمادها في يناير من عام 2008، لتضع ثلاث دعائم أساسية لسياسة الحلف تجاه الفضاء الإلكتروني هي[1]:

- التبعية:

بمعنى تقديم المساعدة عند الطلب، وخلاف ذلك تم تطبيق مبادئ مسؤولية الدولة ذات السيادة.

- عدم التكرار:

بمعنى تفادي التكرار غير الضروري للهياكل والقدرات – على المستوى الدولي والإقليمي والوطني.

1- د. أولاف تايلر، التهديدات الجديدة: الأبعاد الإلكترونية، **مرجع سبق ذكره**، يمكن المطالعة على:
http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/AR/index.htm

- الأمن:

بمعنى التعاون القائم على الثقة مع الأخذ في الاعتبار حساسية المعلومات ذات الصلة، التي يمكن الوصول إليها والمخاطر الممكنة.

ومن ثم أضافت الولايات المتحدة إلى أجهزتها الداخلية الخاصة باستخدامات القوة الإلكترونية، بعداً دولياً جديداً وهو منظمة حلف شمال الأطلنطي، وهو ما يضع القوة الإلكترونية موضع الاستخدام العسكري نظراً للطبيعة التي يتميز بها هذا الحلف.

6- الحرب النفسية الإلكترونية Cyber Psychological Warfare:

حيث قامت القوات الأمريكية إبان الغزو الأمريكي للعراق عام 2003، باختراق الشبكة العسكرية ذات الدوائر المغلقة الخاصة بالجيش العراقي، وأرسلت رسائل من القيادة الأمريكية الوسطى إلى الضباط والجنود العراقيين عبر البريد الإلكتروني، تعلن فيها عزو العراق في المستقبل القريب، وتؤكد أن الهدف هو إزاحة صدام وابنيه من دون إصابة الجنود العراقيين، وتطالب القادة بأن يضعوا المدرعات والدبابات التي تحت إمرتهم في صورة تشكيل ثم يتركوها ويذهبوا إلى بيوتهم، مما يسهل عملية القصف وتدمير هذه التشكيلات، وتعد الضباط والجنود بأن يعودوا إلى مراكزهم من جديد بمجرد إزاحة صدام، وهو ما أثر بالفعل سلبياً على كثير من الجنود، واستجاب قادة عسكريون عراقيون للتعليمات، حيث وجدت القوات الأمريكية العديد من الوحدات وقد اصطفت ودباباتها بانتظام في صفوف أمام قواعدها، مما سمح للطائرات الأمريكية بقصفها قصفاً محكماً[1].

1- ريتشارد كلارك وروبرت نيك، **مرجع سبق ذكره**، ص ص 22-24.

الخلاصة:

مثلت القوة الإلكترونية أحد الأسلحة العسكرية التي يمكن أن تحقق أهدافها بفاعلية، سواء من خلال سرقة المعلومات الاستراتيجية والتلاعب بها، أو استهداف البنى التحتية العسكرية وشبكات الاتصال اللاسلكية للخصوم، ومع ذلك فإن الولايات المتحدة لم تستطع أن تحكم السيطرة كليةً على مجال الفضاء الإلكتروني، كما أنها لا تنفرد بقوة إلكترونية تمكنها من إدارة علاقاتها الخارجية بصورة مستقلة، بل هي تخضع لمجال التأثير والتأثر، فكما تتمكن من التأثير في سياسات الدول من خلال قوتها الإلكترونية، تستطيع أيضاً بعض الدول التي تنافسها في هذا المجال، مثل الصين وروسيا وإيران أو حتى بعض الأفراد العاديين، مثل سنودنوأسانجوالتأثير في السياسة الأمريكية.

ومن ثم يمكن اعتبار الولايات المتحدة قوة إلكترونية لا يمكن الاستهانة بها، ولكنها ليست القوة الوحيدة، وقد استطاعت هذه القوة التمكن من تحقيق بعض الأهداف السياسية والعسكرية، لكنها ليست العامل الحاسم في إدارة علاقتها الخارجية، بل يمكن اعتبارها إحدى الأدوات التي تشترك معها أدوات السياسية الخارجية الأخرى، مثل القوة الاقتصادية والدبلوماسية والعسكرية.

المبحث الثالث

استخدام القوة الإلكترونية الأمريكية في إدارة التفاعلات الدولية الاقتصادية

تتمثل الخطورة الرئيسية في أن الفضاء الإلكتروني أصبح جاذباً لكافة قطاعات المجتمع، أفراداً وجماعات، وأصبح الاعتماد بصورة أساسية على التكنولوجيا الرقمية في تخزين البيانات والمعلومات، واستخدام الحاسب الآلي في تطوير الصناعات وتحريك الاقتصادات، وأصبحت المعاملات المالية والاقتصادية محوسبة، وباتت شبكات البنوك والبورصات وشركات الأسواق المالية مرتبطة عبر بعضها البعض بنُظم وشبكات إلكترونية، فأصبحت التكنولوجيا هي أساس المعاملات المالية والاقتصادية، وشكلت أساس التطور الاقتصادي في القرن الحادي والعشرين، ولعبت الدور نفسه الذي لعبه الفحم في الثورة الصناعية، فأصبح من يمتلك هذه التكنولوجيا يستطيع أن يغير الخريطة الصناعية والاقتصادية، وأن يؤثر في الاقتصاد العالمي.

ممارسة النفوذ الاقتصادي من خلال أدوات القوة الإلكترونية أصبحت توجهاً عاماً لدى كثير من الدول، سواء من خلال سرقة بيانات أو معلومات اقتصادية أو براءات اختراع وخطط تسويقية، أو من خلال التجسس على المسؤولين الماليين والمؤسسات الاقتصادية، كما تلجأ إليها كثير من الشركات بهدف غزو أسواق جديدة أو تحقيق أرباح مالية.

يحلل هذا المبحث كيفية استخدام القوة الإلكترونية في إدارة التفاعلات الاقتصادية الأمريكية، ويحاول خلاله الكاتب معرفة ما إذا كانت القوة الإلكترونية من عناصر القوة الأمريكية التي يمكن من خلالها إدارة العلاقات الاقتصادية بصورة تحقق مصالح الولايات المتحدة الأمريكية، أم أنها مجرد سلاح مزدوج استفادت منه في بعض الجوانب، وسبب لها مشكلات في جوانب أخرى، حيث اعتبر أحد التقارير المقدمة إلى الكونجرس الأمريكي أن التجسس

الاقتصادي على الولايات المتحدة وسرقة المعلومات والأبحاث الخاصة بتطوير الصناعات يعتبر من التهديدات المتزايدة التي تهدد أمن ورفاهية الولايات المتحدة[1]، وقدّر الجنرال إلكسندر كيث المدير السابق لوكالة الأمن القومي الأمريكي NSA الخسائر الاقتصادية التي تترتب على سرقة حقوق الملكية الفكرية وبراءات الاختراع بـ 250 مليار دولار سنوياً، بالإضافة إلى 114 مليار دولار نتيجة للجرائم الإلكترونية[2]، مثل التحويل غير الشرعي للأموال ومحاولات الابتزاز الشخصي وغسيل الأموال عبر الإنترنت وغيرها.

هناك نوعان من الخسائر الاقتصادية التي يمكن أن تترتب على الهجمات الإلكترونية:

- خسائر مباشرة:

تتمثل في تحويل أموال من بنوك، أو سرقة بيانات حول أسعار منتجات أو خطط تسويق أو نتائج أبحاث تم التوصل إليها، مما يؤثر على قدرة الشركات على المنافسة والحصول على المناقصات اللازمة لتنفيذ مشاريع جديدة، حيث تقدم الشركة التي تقوم بعملية التجسس عروضاً أرخص من التي قدمتها نظيرتها المنافسة، مما يترتب عليها حصولها على المناقصة أو العطاء المالي.

1-**Foreign Spies Stealing US Economic secrets in cyberspace**, office of the national counterintelligence executive, October 2011, pi.
2-Josh Rogin, **The Cable NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history,** Foreign Policy: The Cable,on July 12, 2014, onhttp://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history

- **خسائر غير مباشرة:**

تتمثل في سرقة معلومات خاصة برؤية الشركات وقطاع الصناعات المستقبلية، أو قواعد بيانات خاصة بعملاء أو غيرهم، فضلاً عن ارتفاع تكلفة التأمين الإلكتروني، فقد أوضح مكتب الإدارة والميزانية الأمريكي أن ميزانية التأمين الإلكتروني لعام 2012 بلغت 15 مليار دولار أمريكي، لاستثمارها في مشاريع وأنشطة خاصة بالتأمين الإلكتروني، حيث تلجأ الشركات إلى زيادة الانفاق على البنية التحتية الإلكترونية بهدف تأمينها وتطوير النظم الإلكترونية المستخدمة حتى تكون أكثر أماناً، ويمكن تحديد أنماط توظيف القوة الإلكترونية الأمريكية في إدارة العلاقات الدولية الاقتصادية سواء من جانب الولايات المتحدة أو من جانب القوى الدولية الأخرى تجاهها **بالشكل التالي:**

1- تدعيم مكانة الاقتصاد الأمريكي دولياً:

تمثل التكنولوجيا أحد أهم أدوات التقدم الاقتصادي، حيث تعمل على زيادة الناتج الإجمالي على مستوى الاقتصاد الكلي، وتساهم في تحقيق الرفاهية الاقتصادية للشعوب، وتساهم شركات المعلومات وتكنولوجيا الاتصالات في الناتج القومي الأمريكي بنسبة كبيرة، وصلت عام 2011 إلى تريليون دولار، بما يمثل 7.1% من الناتج القومي الأمريكي، تشمل 600 مليار دولار عوائد مباشرة من صناعة المعلومات والاتصالات و400 مليار دولار عوائد غير مباشرة من خلال القطاعات الأخرى المستفيدة[1]. وخلال الفترة من 2001 حتى 2011 ساهم هذا القطاع في خلق وظائف وصلت إلى 565.000 وظيفة بنسبة زيادة 22.2%، وقد نمت الوظائف المتعلقة بهذا القطاع 95 ضعف القطاعات الأخرى[2]، وخلال فترة الأزمة الاقتصادية بين عام 2007 وعام 2011 وانخفاض معدل التوظيف، شهد هذا القطاع زيادة بلغت 6.8%، وقد تستحوذ صناعة تكنولوجيا المعلومات الأمريكية على 26% من حصة هذا القطاع السوقية على مستوى العالمعام 2010، الأمر الذي يجعل الولايات المتحدة أكبر مصدر لهذا النوع من الصناعات[3]، وهو الأمر الذي يساعد على تحقيق الرفاهية الاقتصادية للولايات المتحدة، ويمكنها من فرض سيطرتها على قطاع صناعة الاتصالات دولياً.

1- Robert J. Shapiro and AparnaMathur, **The Contributions of Information and Communication TechnologiesTo American Growth, Productivity, Jobs and Prosperity**, September 2011, on.http://www.tiaonline.org/gov_affairs/fcc_filings/documents/Report_on_ICT_and_Innovation_Shapiro_Mathur_September_8_2011.pdf

2-Bureau of Labor Statistics, **Occupational Employment Statistics** (occupational employment and wage estimates, nationalcross-industry estimates, May 2001, May 2011; accessed July 17, 2014), http://www.bls.gov/oes/oes_dl.htm.

3-**National Science Board, Science and Engineering Indicators 2012**, appendix table 6-13. http://www.nsf.gov/statistics/seind12/pdf/at.pdf

فقد تغير شكل الاقتصاد الأمريكي خلال العشرين عاماً الماضية، فتحولت أصول الشركات من الاعتماد على الأصول المادية Tangible Assets التي تشمل المباني والمعدات والسيارات والأجهزة، إلى الاعتماد على الأصول غير المادية Intangible Assets التي تشمل براءات الاختراع والأسرار التكنولوجية والتجارية وخطط التسويق، وأصبحت تشكل ما يقرب من 80% من أصول الشركات حسب تقديرات شركة ستاندرد آند بورز المتخصصة في التحليلات المالية[1].

1-Protecting Key Assets:A Corporate Counterintelligence Guide,**Op.cit**, p 2, Onhttp://www.ncix.gov/publications/reports/fecie_all/ProtectingKeyAssets_CorporateCIGuide.pdf

2- جمع معلومات اقتصادية استخباراتية Economic Intelligence:

لعبت التكنولوجيا دوراً مهماً في تطوير كثير من الصناعات، بل أصبحت صناعة التكنولوجيا محركاً رئيسياً ليس للاقتصاد المحلي فحسب، بل والاقتصاد العالمي أيضاً، وعلى الرغم مما وفرته من سرعة في الأداء وتوفير في الوقت والجهد وتقليل النفقات، فإنه كان لها بعض الجوانب السلبية، حيث أصبحت معظم الصناعات والعمليات المالية التي يدخل في تكوينها الجانب الإلكتروني عرضة للسرقة من خلال عمليات القرصنة والاختراق.

وقد انعكس التطور التكنولوجي بصورة كبيرة على تطوير أدوات التجسس المالي والاقتصادي، فلم تعد محاولات التجسس الاقتصادي تقليدية من خلال جمع معلومات عبر المواقع الإلكترونية للشركات أو تجنيد أحد موظفي الشركة أو حتى عمل دراسات ميدانية للأسواق لجمع المعلومات، بل يمكن اختراق شبكة المعلومات الخاصة بالشركة المستهدفة، لمعرفة ميزانيتها وعدد موظفيها ومراحل إعداد المنتج وبراءات الاختراعات التي حصلت عليها وأسرار تطوير صناعتها وقواعد بيانات عملائها وخططها التسويقية واستراتيجيتها التفاوضية مع عملائها، من دون وجود خسائر كبيرة تذكر، فقد يحدث ذلك وتمر السنوات من دون أن تدرك الشركة المستهدفة أنها ضحية لعملية اختراق، وحتى إذا أدركت، فهناك صعوبة في تحديد مصدر الهجمات الحقيقي، كما أن الشركات الكبرى التي تتعرض للاختراق وسرقة المعلومات، قد لا تستطيع أن تعلن ذلك في وسائل الإعلام أو حتى تقوم بإبلاغ الأجهزة الرسمية والقانونية للحفاظ على منتجاتها من السرقة، وذلك من أجل الحفاظ على صورتها أمام عملائها سواء كانوا من داخل الحكومة أو من خارجها، كما أن بعض الشركات التي تتعرض لعمليات اختراق إلكتروني تخشى من اتهام قراصنة يتبعون حكومات أو شركات أخرى بمحاولة اختراق وسرقة معلومات خاصة بها، حتى تحافظ على وجودها في أسواق هذه الدول.

وتعاني الولايات المتحدة من اختراق شبكات الشركات الأمريكية عبر الفضاء الإلكتروني، بهدف سرقة المعلومات التجارية، وبراءات الاختراعات، وأسرار التكنولوجيا المتقدمة من شبكات وأجهزة الشركات العاملة في هذا المجال، وهو ما

يخدم أهداف الدول والشركات التي تقوم بعملية الاختراق، بما يساعد على تطوير منتجاتهم وإضعاف قدرة المنتجات الأمريكية على المنافسة بسبب تقليدها أو حتى سرقتها وتطويرها، وعادة ما يتم استهداف المعلومات الاقتصادية والتكنولوجيا الأمريكية من خلال أجهزة استخبارات، وشركات خاصة، ومعاهد بحثية وأكاديمية، والعديد من الأفراد سواء كانوا يعملون لدى جهات أو يعلمون منفردين.

وتعتبر كل من الصين وروسيا أبرز القراصنة الإلكترونيين الذي يعلمون على جمع معلومات اقتصادية استخباراتية أمريكية، حيث صنف تقرير صادر من مكتب مكافحة التجسس الصين بأنها أكثر الدول نشاطاً واستمراراً في عمليات القرصنة الإلكترونية على مستوى العالم، كما تجري أجهزة الاستخبارات الروسية العديد من العمليات على الفضاء الإلكتروني بهدف جمع معلومات اقتصادية وتكنولوجيا أمريكية تخدم المصالح الروسية وتساعد في ازدهار الاقتصاد الروسي وتقدمه تكنولوجيا من خلال جمع معلومات استخباراتية اقتصادية.

وكذلك يقوم بعض حلفاء الولايات المتحدة وشركائها باستخدام قدرتهم على التواصل مع المعاهد والمراكز البحثية الأمريكية للحصول على هذه المعلومات بما يدعم قدرتهم الاقتصادية[1]، ويعتبر هذا التقرير بمنزلة أحد أول الوثائق التي الرسمية التي تتهم فيها الولايات المتحدة كلاً من الصين وروسيا صراحةً بشن هجمات إلكترونية عليها بهدف سرقة معلومات اقتصادية.

ولما كانت الولايات المتحدة لاعباً أساسياً في قلب النظام الاقتصادي الدولي، ومحرك رئيسي في تطوير التكنولوجيا الحديثة، فإن اقتصادها دائماً في موضع للخطر وعرضه للاختراق والقرصنة، بهدف جمع المعلومات الاقتصادية والصناعية التي تتحكم في الأسواق العالمية، وكلما زادت محاولات التأمين الإلكتروني، فإن أساليب القرصنة الإلكترونية تتطور وتزداد.

1-**Foreign Spies Stealing US Economic secrets in cyberspace**, office of the national counterintelligence executive, October 2011, pi.

وقد نشرت مجلة التايم تقريراً حول تعرض كبريات شركات الصناعة الأمريكية لسلسة من الهجمات الإلكترونية مصدرها الصين باسم "مطر العمالة Titan Rain"بدأت منذ 2003[1]، وقد أكد تقرير مانديات Mandiant– إحدى شركات الأمن الإلكتروني الأمريكية– لعام 2013 أن الصين قد هاجمت على الأقل 141 مؤسسة صناعية أمريكية في بداية عام 2006 وترتبت عليها سرقة تيرابابيتس Terabytes من البيانات وبراءات الاختراع وحقوق الملكية الفكرية ونتائج أبحاث علمية وأسعار منتجات جارٍ تسويقها وقواعد بيانات العملاء، فقد شملت 20 نوعاً من صناعات مختلفة[2]، مما ألحق خسائر اقتصادية بهذه الشركات صبت في مصلحة الاقتصاد الصيني على حساب الاقتصاد الأمريكي.

وفي فبراير 2011 أشار تقرير صادر عن شركة "مكافيMacAfee" المتخصصة في برامج مكافحة الفيروسات إلى تعرض كبريات شركات النفط الأمريكية وشركات الطاقة والبتروكمياويات إلى هجمات إلكترونية ترجع إلى IP جهاز كمبيوتر يوجد بالصين عام 2009[3]، كما يؤكد تقرير صادر من مجلس السياسة الخارجية الأمريكية American Foreign Policy Council أن الصين تستخدم الإنترنت من أجل التجسس على مختلف الحكومات، خاصة الأمريكية، فتقوم بجمع معلومات استخباراتية اقتصادية، والتجسس على العمليات المخابراتية، فضلاً عن التحكم في تدفق البيانات عبر شبكات الكمبيوتر ومراقبة أنشطة المواطنين[4].

وقد أوضح التقرير المقدم إلى الكونجرس أن أجهزة الاستخبارات الصينية تعمد إلى استغلال الأشخاص ذوي الأصول الصينية داخل الشركات الأمريكية الكبرى، بهدف سرقة بعض المعلومات الاستراتيجية من خلال البريد الإلكتروني أو أجهزة

1- Nathan Thornburgh,Inside the Chinese Hack Attack, **Time**, on July 12th,2014. http://content.time.com/time/nation/article/0,8599,1098371,00.html
2-**Exposing one of china's cyber espionage unites**, Mandiat report, APT-1,Feb 2013, p1, on http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
3-**Global Energy Cyberattacks:"Night Dragon"**, McAfee® Foundstone® Professional Services and McAfee Labs™, February 10th, 2011, P3.
4-Larry Wortzel, **Defense dossier**, American Foreign Policy Council, August 2012, p1.

محمولة Portable Devices[1]، حيث تم الحكم في عام 2010 في 7 قضايا تجسس اقتصادي كانت منهم 6 قضايا ذات صلة بالصين[2]. وفي مايو 2014 وجهت الحكومة الأمريكية اتهاماً رسمياً لخمسة جنود في الجيش الصيني بسبب اختراقهم مواقع وأجهزة شركات أمريكية كبرى تعمل في الصين بين عامي 2006 - 2014، حيث قام القراصنة باختراق وسرقة بيانات وتصاميم سرية، تعود لشركات أمريكية كانت تعمل في الصين، ومنها شركة "ويستنجهاوس"، التي كانت متعاقدة لبناء أربع محطات لتوليد الطاقة في الصين، وشركة "سولار وورلد" للطاقة الشمسية، وشركة الحديد الأمريكية، وشركة "الكوا للألمنيوم"[3].

وتواجه الصين الاتهامات الأمريكية بإنكار تام، وتؤكد أنها أيضاً ضحية لعمليات اختراق إلكتروني، وهو أمر صعب الحدوث، وإن كان وارداً، نظراً لأن الصين تأخذ موضوع الأمن الإلكتروني بجدية تامة، فيمكن للحكومة الصينية أن تفصل الصين عن الشبكة العالمية للإنترنت في حال تعرضها لأي هجوم إلكتروني، كما أكدت شركة "مايكروسوفت" في تقرير صادر على مدونتها الإلكترونية أن الصين هي أقل الدول تعرضاً للإصابة ببرمجيات خبيثة[4].

وحينما حاولت شركة كوكاكولا الأمريكية أن تستحوذ على مجموعة "هوييوان" الصينية للعصائر بمبلغ قدره 2.4 مليار دولارٍ، عام 2009، في أكبر عملية للاستحواذ على شركة صينية، قام قراصنة صينيون من خلال التصيُّد الإلكتروني Phishing بإرسال رسائل بريد إلكتروني عشوائية بها روابط تحمل برامج اختراق، للإيقاع بأحد مسؤولي الشركة حينما قام بالضغط على أحد الروابط التي تحتوي برمجيات خبيثة، فاستطاع القراصنة اختراق شبكة الشركة بهدف الحصول على

1-Foreign Spies Stealing US Economic secrets in cyberspace, **Op Cit**, p5.

2-Ibid**.**

3- أمريكا تتهم الجيش الصيني بالتجسس الاقتصادي، **موقع العرب اليوم**، بتاريخ مطالعة 5 أغسطس 2014، يمكن المطالعة على:

:http://alarabalyawm.net/?p=195886

4-Tim Rains, **the threat landscape in china: A Pradox**, March 2012, on July 23th,2014. http://blogs.technet.com/b/security/archive/2013/03/11/the-threat-landscape-in-china-a-paradox.aspx

الوثائق الخاصة باستراتيجية التفاوض للاستحواذ على الشركة الصينية، للوصول إلى أفضل الأسعار[1].

وإذا كانت الولايات المتحدة ضحية للهجمات الإلكترونية ذات الطبيعة الاقتصادية فهي في الوقت نفسه جانية وسارقة لبيانات اقتصادية، حيث نشرت صحيفةكريستي انساين سمونيتور وصحيفة الجارديان تقارير سربها سنودن تؤكد تجسس وكالة الأمن القومي الأمريكي على شركات برازيلية، خاصة شركة النفط الحكومية في البرازيل وهي شركة "بتروبراس"، التي تملك اكتشافات نفطية كبيرة، وهو من شأنه بالتأكيد أن يؤثر على مصالح النفط الأمريكية البرازيلية المشتركة[2].

ونتيجة لعمليات التجسس الاقتصادي التي تقع فيها العديد من الشركات والمؤسسات الاقتصادية والصناعية ضحية لعمليات قرصنة إلكترونية.

قدم مكتب التحقيقات الفيدرالي الأمريكي عدة توصيات لهم لتفادي وقوعهم ضحايا سرقة أو نصب إلكتروني، يمكن تلخيصها في التالي[3]:

- إدراك الشركة بوجود تهديد ما لمصالحها الاقتصادية Recognize The Threat

- تحديد الأسرار التجارية وتصنيفها من حيث أهميتها Identify And Value Trade Secrets

1-DAVID E. SANGER, Chinese Army Unit Is Seen as Tied to Hacking Against U.S, **The New York Times**, February 18, 2013, Accessed on July 10th, 2014, on http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?hp&_r=1&pagewanted=all&

2-Jonathan Watts,NSA accused of spying on Brazilian oil company Petrobras,**The Guardian**, September 9, 2013, Accessed on 30 June 2014, on http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras

3-**Economic Espionage: Protecting American's Trade Secrets,** FBI, on July 3, 2014, on http://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage

- وضع خطة تأمين محكمة للأسرار التجارية للشركات

Plan For Safeguarding Trade Secrets

- تحديد الأشخاص المسموح لهم بالولوج عبر النظم الإلكترونية إلى الأسرار التجارية.

- تأمين الأسرار التجارية المادية، والتي قد تكون أوراقاً أو مواد كيمائية تم تصنيعها أو غيرها.

- تنظيم تدريب أمني باستمرار للعاملين بالشركات بهدف التوعية الأمنية من مخاطر سرقة البيانات.

- تصميم نظام إلكتروني أمني داخلي قادر على اكتشاف مصادر التهديد، والعمل على تطويره وتحديثه باستمرار.

- إبلاغ مكتب التحقيقات الفيدرالي عن أي حوادث مشبوهة بسرقة بيانات مهمة.

3- التجسس على المسؤولين والمؤسسات المالية:

من الأدوات التي يمكن أن تمارس بها الولايات المتحدة قوتها الاقتصادية التجسس على المسؤولين الماليين بهدف معرفة مواقف الدول تجاه بعض القرارات والمواقف الاقتصادية، حيث كشفت تسريبات سنودن عن قيام الحكومة الأمريكية بالتجسس على وزير المالية التركي أثناء اجتماع وزراء المالية لمجموعة العشرين G20 في لندن في سبتمبر 2009 بهدف معرفة موقف تركيا من التعاون مع بقية دول المجموعة، فالحكومات لا تعتمد فقط على تقييم وتحليل الخطابات والمفاوضات والتحركات السياسية الظاهرة من أجل تقدير المواقف السياسية والاقتصادية لنظرائها من الحكومات، بل تلعب المخابرات دوراً يساعد على استباق الأحداث، ومن ثم اتخاذ السياسات التي تصب في مصلحتها أولاً وبشكل أسرع في مواجهة الحكومات الأخرى[1].

ولما كانت واشنطن مقراً مالياً للمؤسسات المالية الكبرى، خاصة البنك الدولي وصندوق النقد الدولي فإنها لم تخل أيضاً من محاولات التجسس الأمريكي عليها، حيث نشر موقع رويترز خبراً يؤكد قيام الرئيس الأمريكي باراك أوباما بإصدار أوامر بوقف التنصت على مقري صندوق النقد الدولي والبنك الدولي، وذلك في إطار مراجعة لأنشطة جمع المعلومات الاستخباراتية[2]، بعد تسرب أخبار عن تجسس وكالة الأمن القومي على هذه المؤسسات.

1- كريم خشبة، **تسريبات سنودن: إدارةالعلاقات الدولية في عصر التسريبات**، تحليل منشور على موقع المركز الإقليمي للدراسات الاستراتيجية، بتاريخ 1 يوليو 2014، يمكن المطالعة على:

http://www.rcssmideast.org/%D8%A7%D9%84%D8%A5%D8%B5%D8%AF%D8%A7%D8%B1%D8%A7%D8%AA/%D8%AD%D8%A7%D9%84%D8%A9-%D8%A7%D9%84%D8%B9%D8%A7%D9%84%D9%85/%D8%AA%D8%B3%D8%B1%D9%8A%D8%A8%D8%A7%D8%AA-%D8%B3%D9%86%D9%88%D8%AF%D9%86.html

2- أوباما أمر بوقف تجسس وكالة الأمن القومي على مقري صندوق النقد الدولي والبنك الدولي، **موقع رويترز**، بتاريخ 1 نوفمبر 2013، بتاريخ دخول 1 يوليو 2014، يمكن المطالعة على:

http://ara.reuters.com/article/worldNews/idARACAE9B2C3S20131101

4- تحويل غير شرعي للأموال:

تعاني الولايات المتحدة وغيرها من دول العالم من القرصنة الإلكترونية على المصارف والمؤسسات المالية، حيث يقوم بعض القراصنة بتحويل مئات الآلاف وفي بعض الأحيان ملايين من الدولارات من حسابات بنكية إلى حساباتهم الخاصة، وقد تميزت هذه العصابات الإلكترونية بقدرتها على تجميع أفرادها عبر دول مختلفة، مما يجعل عملية تعقب الأموال وأفراد العصابة غاية في الصعوبة.

ومن الأمثلة على هذه العصابات التي استطاعت تحويل أموال من بنوك أمريكية، عصابة تتكون من مصريين وأمريكيين، حيث قامت قوات الأمن المصرية بالتعاون مع نظيرتها الأمريكية في أكتوبر 2009 بالقبض على مجموعة قراصنة من طلاب جامعات ومعاهد مصرية بالإضافة إلى متهمين آخرين في الولايات المتحدة، ووجهت إليهم تهم القرصنة الإلكترونية وتحويل غير شرعي لأموال من بنكي أوف أمريكا وويلز[1]. وفي يناير 2013 تمكنت الشرطة التايلندية بالتعاون مع مكتب التحقيقات الفيدرالي FBI من القبض على الهاكر الجزائري حمزة بن دلاج الذي يبلغ من العمر 24 عاماً، وعلى الرغم من صغر سنه، فإنه صنف من ضمن أقوى 10 قراصنة مطلوبين من قبل مكتب التحقيقات الفيدرالي حيث تتهم السلطات الأمريكية ابن دلاج بدخول مواقع حسابات مصرفية خاصة في أكثر من 217 بنكا وشركة مالية في أرجاء العالم، والتسبب في فقدان ملايين الدولارات[2].

ومن الأمثلة على التحويل غير الشرعي للأموال وسرقتها تمكّن بعض القراصنة من اختراق مجموعة (سيتي جروب) الأمريكية 2009، وسرقة عشرات الملايين من الدولارات، مما أصاب النظام الاقتصادي الأمريكي بخسائر فادحة، وهذا الفعل تبين بعد ذلك أنه تم بالتنسيق بين مجموعة من القراصنة الأمريكيين بعصابة روسية من خلال شبكة الإنترنت[3].

1- محاكمة جنائية لأكبر شبكة غسيل أموال في مصر وأمريكا، **بموقع الأهرام الرقمي**، بتاريخ 9 فبراير 2010، بتاريخ دخول 2 يوليو 2014، يمكن المطالعة على:

http://digital.ahram.org.eg/articles.aspx?Serial=57999&eid=1387

2- تايلاند تقبض على "قرصان البنوك" الجزائري حمزة بن دلاج، **موقع BBC**، تاريخ 8 يناير 2013، بتاريخ 8 يناير 2013، تاريخ دخول 8 أغسطس 2014، يمكن المطالعة على:

http://www.bbc.co.uk/arabic/worldnews/2013/01/130108_thailand_algeria_usa_bank_hacking.shtml

3- شيريهان نشأت المنيري،الإرهاب الإلكتروني، **موقع السياسة الدولية**، بتاريخ دخول 10 سبتمبر 2013، يمكن المطالعة على:

http://www.siyassa.org.eg/UI/Front/InnerPrint.aspx?NewsContentID=2450

5- استهداف مواقع البنوك والشركات وقواعد البيانات:

يلجأ بعض القراصنة إلى مهاجمة مواقع البنوك والشركات بهدف سرقة بيانات خاصة بالعملاء أو بطاقات ائتمان أو الاكتفاء بتعطيل خدمات البنك الإلكترونية، من خلال هجمات الحرمان من الخدمة Denial Of Service Attack.

وقد تعرضت الولايات المتحدة لواحدة من هذه الهجمات في أواخر عام 2011 وبلغت ذروتها في سبتمبر 2012، حيث رجح مسؤولون أمريكيون وقوف إيران خلف هجمات إلكترونية واسعة النطاق استهدفت قطاع المصارف والنفط بالولايات المتحدة، وأصابت المؤسسات المالية الأمريكية[1]، وتسببت في عدم القدرة على الولوج للحسابات المصرفية.

فضلاً عما تطلبته من إجراءات مواجهة باهظة الثمن، **كما أصابت الهجمات أكثر من 12 مؤسسة رئيسية منها:**

SunTrust, JPMorgan Chase, Citi Group, Well Fargo, U.S. Bancorp,) (Capital One, PNC, HSBC, BB&T[2]،هذا فضلاً عن إنفاق البنك الواحد ما لايقل عن 10 ملايين دولار للتخفيف من أثر الهجمات[3]، وقد جاء ذلك رداً على استهداف البرنامج النووي الإيراني من خلال فيروسي ستاكسنت Stuxnet وفيلم Flame.

1- خبراء: الحرب الإلكترونية أخطر تهديد إيراني، **موقع CNN**، تاريخ 7 نوفمبر2012، بتاريخ مطالعة 9 سبتمبر 2012، يمكن المطالعة على:

http://arabic.cnn.com/2012/scitech/11/6/_iran-cyberattack/index.html

2-**Exclusive: Iranian hackers target Bank of America, JPMorgan**, Citi, On July 3, 2014http://www.reuters.com/article/2012/09/21/us-iran-cyberattacks-idUSBRE88K12H20120921

3- محمد الحسين، **الحرب الافتراضية: هل تملك طهران القدرة على مهاجمة واشنطن الكترونيا؟** المركز الإقليمي للدراسات الاستراتيجية، بتاريخ مطالعة 10 سبتمبر 2013، يمكن المطالعة على الرابط التالي:

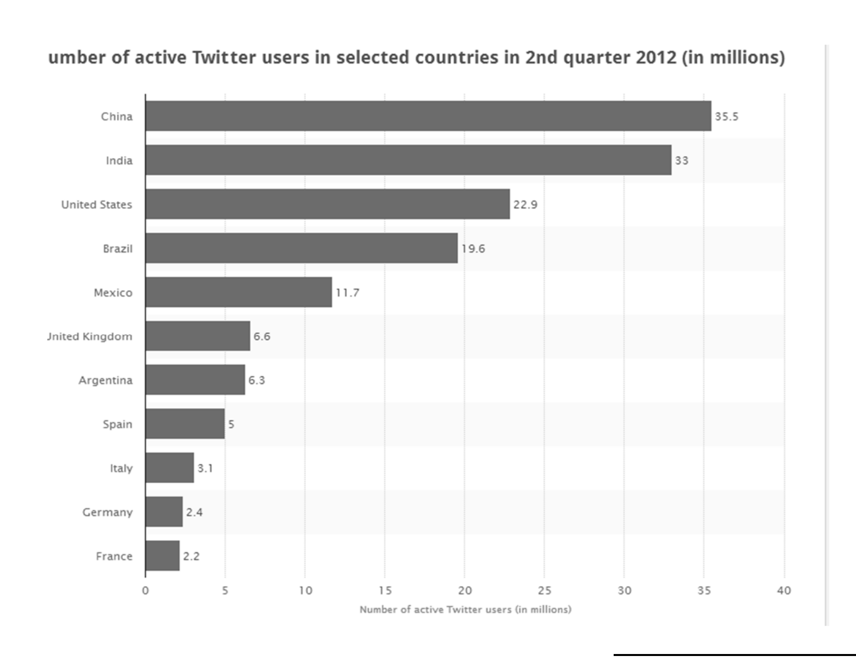
http://rcssmideast.org/%D8%A7%D9%84%D8%AA%D8%AD%D9%84%D9%8A%D9%84%D8%A7%D8%AA/%D8%A7%D9%84%D8%A3%D9%85%D9%86%D8%A7%D9%84%D8%A3%D9%82%D9%84%D9%8A%D9%85%D9%89/%D8%A7%D9%84%D8%AD%D8%B1%D8%A8D8%A7%D9%84%D8%A7%D9%81%D8%AA%D8%B1%D8%A7%D8%B6%D9%8A%D8%A9.html

وقد أصدر فريق الاستجابة للطوارئ عبر الإنترنت في أنظمة التحكم الصناعي بوزارة الأمن الداخلي The Industrial Control Systems Cyber Emergency Response Team تقريره ربع السنوي، ليؤكد فيه تزايد الهجمات الإلكترونية التي تتعرض لها مختلف القطاعات الاقتصادية بالولايات المتحدة بنسبة 52% في الربع الأخير من عام 2012[1].

1- **ICS-CERTMONITOR**، U.S. Department of Homeland Security cybersecurity response team, Dec 2012, On https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2012.pdf

6- مساندة الشركات التكنولوجيا العملاقة:

نشبت عدة صراعات بين عدد من الشركات الأمريكية العملاقة وبعض الحكومات مثل شركة فيس بوك وجوجل وتويتر وغيرها من الشركات العاملة في مجال تكنولوجيا المعلومات، وقد شهد ذلك تدخلاً في بعض الأحيان من جانب حكومة الولايات المتحدة، إما دفاعاً عن مصالح هذه الشركات، أو عن مبدأ حرية الرأي والتعبير، فخلال الصراع بين الحكومة الصينية وجوجل عام 2010 قالت وزيرة الخارجية الأمريكية هيلاري كلينتون في بيان لها أن الولايات المتحدة لديها مخاوف خطيرة بشأن اتهامات من جوجل بأن الصين تمارس رقابة على نتائج البحث على الإنترنت وبطريقة أخرى تتدخل في الحريات على الإنترنت، مشيرة إلى أن شركة جوجل أخطرت الإدارة الأمريكية بهذه المزاعم التي تثير مخاوف خطيرة جداً[1]، وهو الأمر الذي لم تتقبله الحكومة الصينية،فقامت بإدانة سياسة الولايات المتحدة إزاء الإنترنت واتهمتها بالسعي لتحقيق الامبريالية المعلوماتية.



1- كلينتون: قضية جوجل في الصين تثير مخاوف خطيرة، **وكالة رويترز للأنباء**، بتاريخ مطالعة 1 أغسطس 2014، يمكن المطالعة على:

http://ara.reuters.com/article/idARACAE60C05720100113

وعلى الرغم من أن الصين تحظر استخدام تويتر داخلها منذ عام 2009 بالإضافة إلى الفيس بوك ويوتيوب، فإنها أعلى الدول استخداماً له، وذلك بواقع 35.5 مليون مستخدم حتى الربع الأخير من عام 2012[1]، حيث يلجأ المستخدمون إلى أدوات مثل VPN لتجاوز الحجب، ويمكن أحياناً نشر التغريدات عبر تطبيقات خارجية مثل Tweet Deck وغيرها.

1- Number of active Twitter users in selected countries in 2nd quarter 2012 (in millions),On 23 Oct 2014 , http://www.statista.com/statistics/242606/number-of-active-twitter-users-in-selected-countries/

الخلاصة:

مما سبق، يتضح أن ممارسة النفوذ الاقتصادي من خلال أدوات القوة الإلكترونية أصبح توجهاً عاماً لدى كثير من الدول، سواء من خلال سرقة بيانات أو معلومات اقتصادية أو براءات اختراع وخطط تسويقية، أو من خلال التجسس على المسؤولين الماليين والمؤسسات الاقتصادية، كما تلجأ إليها كثير من الشركات بهدف غزو أسواق جديدة أو تحقيق أرباح مالية، وقد استخدمت الولايات المتحدة هذه الأداة لتحقيق مكاسب مالية واقتصادية، إلا أنها كانت أيضاً ضحية لعلميات سرقة ونصب إلكتروني، وألحقت خسائر قُدرت بالمليارات من الدولارات سنوياً، مما يجعل عمليات التأمين الإلكتروني للمؤسسات المالية والاقتصادية في غاية الأهمية، فالتكلفة المالية التي قد تترتب على هجمات إلكترونية ذات طبيعة اقتصادية يمكن أن تتسبب في خسائر مالية كبيرة للشركات والبنوك، وتعتبر استنزافاً لموارد الدولة.

وعلى الرغم من تقدم الولايات المتحدة الأمريكية في مجال القوة الإلكترونية، وتوظيفها في إدارة علاقاتها السياسية والعسكرية، فإن قدرتها على توظيفها في المجالات الاقتصادية أضعف من سابقيها، وذلك بسبب اعتماد الاقتصاد الأمريكي على الأصول غير المادية التي في أساسها معلوماتية، وتعرضها لعمليات قرصنة إلكترونية مستمرة، خاصة من الصين وروسيا، مما يشكل نقطة ضعف تواجه الاقتصاد الأمريكي، وتمثل ثغرة تسمح بانتقال السيولة النقدية والصناعات التكنولوجية منها إلى غيرها من الدول، وتخصم من رصيد ازدهار الاقتصاد الأمريكي لصالح دول وشركات أخرى.

الخاتمه:

- **لم تعد الأشكال التقليدية للقوة ثابتة**، ولم تعد مصادرها محددة، بل تغيرت خلال فترة زمنية قصيرة بفعل التقدم التكنولوجي، فكما أن الفحم كان له تأثير على تغير الصناعات، سواء مدنية أو عسكرية، فإن للتكنولوجيا الأثر نفسه، وقد كان لاختراع الفضاء الإلكتروني، بما تميز به من سهولة في الاستخدام ورخص في التكلفة وسرعة ربط الأفراد والشبكات، أثر كبير في تغير موازين القوى، اقتصادياً وعسكرياً، وأصبح لمن يمتلك هذه التكنولوجيا وقادر على تصنيعها وتطويرها، الدور الأبرز في التأثير على الأحداث السياسية والاقتصادية والعسكرية، وقد أثر ذلك على المفاهيم التقليدية للقوة وتحولاتها وتطبيقاتها وأشكالها، فظهر نوع جديد هو القوة الإلكترونية، التي تعتمد على أدوات الاتصال الحديثة والبرمجيات الرقمية المرتبطة بالفضاء الإلكترونية لتحقيق أهدافها، ونتيجة لذلك ظهرت العديد من المفاهيم الجديدة التي تتلاءم مع هذا النوع من القوة، مثل الحرب الإلكترونية والاستخبارات الإلكترونية والتجسس الإلكتروني والدبلوماسية الإلكترونية، وغيرها من المصطلحات التي تؤسس لهذا النوع الجديد من القوة.

- **وقد اهتم الكاتب بدراسة استخدامات الولايات المتحدة الأمريكية للقوة الإلكترونية**، لما تتميز به من قدرات إلكترونية متقدمة، فمعظم الشركات الكبرى المصدرة للتكنولوجيا، مثل جوجل وآبل ومايكروسوفت وفيس بوك وتويتر وغيرها هي شركات أمريكية، فضلاً عن الدور الذي تلعبه وكالة الأمن القومي الأمريكي في تطوير القدرات الإلكترونية الأمريكية، الأمر الذي مكنها من التجسس على ملايين من البشر والرؤساء حول العالم، بالإضافة إلى الدور الكبير الذي توليه استراتيجيات الأمن القومي الأمريكي لهذا النوع من القوة.

- **ولقيام الكاتب بهذه المهمة استخدم منهجاً تم تطويره من جانب فريق عمل تابع لجامعة الدفاع الوطني الأمريكية** لدراسة أثر الفضاء الإلكتروني على الأمن القومي الأمريكي، ويأخذ المنهج شكلاً هرمياً،فيتكون من ثلاثة مستويات، يمثل المستوى الأول البنية التحتية الإلكترونية، وهي تمثل قاعدة الهرم، وتتمثل في المكونات والأدوات التي تستخدمها هذه البيئة، سواء كانت مكونات مادية Hardware أو برمجية Software، فضلاً عن الاستراتيجيات ونظم الاتصالات والعناصر البشرية، ويمثل المستوى الثاني دعائم القوة Levers of Power ، حيث يشهد هذا المستوى تفاعل القوة الإلكترونية الناتجة من المستوى الأول مع الأبعاد الناعمة والصلبة للقوة، وتأتي على قمة الهرم الكيانات التي من المفترض أن تُمكنهم Empowerment مخرجات المستوى الثاني، وقد تكون هذه الكيانات أفراداً أو شركات أو دولاً أو منظمات أو جماعات إرهابية أو إجرامية.

- **وقد تم تطبيق المنهج المستخدم في الدراسة على الولايات المتحدة الأمريكية**، من خلال معرفة عناصر القوة الإلكترونية الرئيسية التي تعتمد عليها الولايات المتحدة، من برامج وأدوات، بالإضافة إلى الوقوف على المصالح الأمريكية داخل الفضاء الإلكتروني، وكيفية تعامل الولايات المتحدة معها، وتحديد أبرز التهديدات التي تواجهها، وكيفية توظيف القوة الإلكترونية في إدارة التفاعلات الأمريكية سواء كانت سياسية أو عسكرية أو اقتصادية، وتحديد ما إذا كانت القوة الإلكترونية إحدى الأدوات الفاعلة في السياسة الخارجية الأمريكية أم لا، وهل استفادت الولايات المتحدة منها استفادة مطلقة، أم كانت سلاحاً مزدوجاً استفادت منه في بعض الأحيان وأصابها في أحيان أخرى، وقد توصل الكاتب إلى عدد من المحددات الرئيسية التي مثلت عائقاً أمام الولايات المتحدة لتوظيف قوتها الإلكترونية بصورة كاملة، ومن خلال تطبيق المنهج المستخدم تمت الإجابة على التساؤل الرئيسي الذي تطرحه المشكلة البحثية وهو "**كيف تستخدم الولايات المتحدة قوتها الإلكترونية في إدارة تفاعلاتها الدولية في الفترة من 2001 حتى 2012؟**"، والتفاعلات هنا تشمل الفعل ورد الفعل على حد سواء.

- **كما تم تطبيق نموذج ناي للاستخدامات الصلبة والناعمة للقوة الإلكترونية في التفاعلات الدولية**، والتي شملت التأثير في سلوكيات الفاعل الدولي ودفعه للقيام بأعمال لم يكن ليقوم بها، وهو الذي حدث في الحالة الإيرانية حينما تم شن هجمات فيروس ستاكسنت على البرنامج النووي الإيراني بغرض تعطيل عمله ولو مؤقتاً، كما تم استخدامها أيضاً للتحكم في أجندة الآخرين من خلال إقصاء استراتيجياتهم حينما دشنت سفارة إلكترونية لتزويد الإيرانيين بمعلومات حول التأشيرات عبر الإنترنت والتواصل مع الطلاب الإيرانيين، كما تم توظيفها في ترتيب أولويات الفواعل الأخرى باتخاذ عدة إجراءات ضد شركات بطاقات الائتمان لمنع ممارسة القمار عبر الإنترنت.

- **كما تمت الإجابة عن الأسئلة البحثيةالتي تم طرحها خلال الدراسة،** وفيما يتعلق بالتساؤل البحثي الخاص بعناصر القوة الإلكترونية والفاعلين الرئيسيين في استخدامها، فنجد أن عناصرها الرئيسية تتمثل في وجود بنية تحتية تكنولوجية متطورة، مع عناصر بشرية قادرة على استخدام هذا النوع من التكنولوجية وتطويره، وابتكار أسلحة إلكترونية سواء هجومية تعمل على تحقيق الأهداف الاستراتيجية للدولة، أو دفاعية تعمل على صد أي هجوم إلكتروني عليها، حتى تصل للردع الإلكتروني، فضلاً عن وجود إطار تشريعي وقانوني يسمح باستخدام القوة الإلكترونية بصورة شرعية، مع وجود هيكل مؤسسي قادر على تحقيق أهداف الدولة من خلال توظيف أدوات القوة الإلكترونية،

- **ويمكن الحكم أن دولة ما تتمتع بقدرات إلكترونية متقدمة من خلال النظر على عدة متغيرات رئيسية تتمثل في وجود التالي:**

- خطة استراتيجية خاصة برؤية الدولة لتعظيم قدرتها الإلكترونية.

- جهة مختصة بالدفاع عن الشبكة الإلكترونية للدولة وحمايتها والعمل على تطويرها.

- بنية تحتية تكنولوجية Cyber Infrastructure، مع الاهتمام بتطويرها وتحديثها بصفة مستمرة.

- شراكات مع القطاع العام والخاص لميكنة النظم والخدمات، وعمل استراتيجيات لتأمينها.

- قوانين تحافظ على الخصوصية، وتمنع ارتكاب الجرائم الإلكترونية.

- نظام تعليمي متقدم يدعم الابتكار ويعتمد على التكنولوجيا المتقدمة.

- عناصر بشرية متدربة وقادرة على استخدام التكنولوجيا الحديثة.

- تطوير أسلحة إلكترونية Cyber weapons تمكن الدولة من تحقيق أهدافها.

- قدرة الدولة على إدارة عمليات إلكترونية (CNO) Computer Network Operations تشمل مهاجمة شبكات الحاسب الآلي إذا دعت الحاجة إلى ذلك، والدفاع عن شبكاتها الخاصة، واستطلاع Exploitation الشبكات الأخرى.

وفي إجابة عن التساؤل البحثي الخاص بأثر ثورة المعلومات على انتشار القوة في السياسة الدولية، نجد أنها ساهمت في انتشار القوة الإلكترونية بين عدد كبير من الفاعلين سواء من الدول أو من غير الدول، وذلك بسبب رخص تكلفتها وسهولة استخدامها وما تتميز به من خاصية التخفي والقدرة على إصابة الأهداف الاستراتيجية للدولة، ومع ذلك يمكن القول إن الدولة مازالت هي الفاعل الرئيسي في هذا المجال، بما تمتلكه من قدرات مالية وتكنولوجية تمكنها من تخصيص مشاريع عملاقة تعمل على تطوير قدرات إلكترونية، سواء كانت هجومية أو دفاعية، ولكن هذا لا يعني أنها الفاعل الوحيد أو المحتكر الفعلي لهذا النوع من القوة، فيشاركها فيها الأفراد، سواء كانوا تنظيمات رسمية أو غير رسمية أو حتى فرادى، ويندرج في هذا النطاق المحترفون والهواة، بالإضافة إلى الحركات الإرهابية والعصابات المنظمة وجماعات الضغط والتنظيمات العرقية والإثنية والشركات والمنظمات الدولية والإقليمية وأي فاعل آخر، سواء كان دولياً أو من غير الدول قادراً على توظيف أدوات التكنولوجيا الحديثة.

وفي الوقت الذي يمثل فيه الفضاء الإلكتروني أهمية كبيرة للولايات المتحدة، نظراً لارتباط معظم البنى التحتية المدنية والعسكرية بالفضاء الإلكتروني، والاعتماد عليه في تقديم معظم الخدمات، سواء حكومية أو غير حكومية للجمهور، إلا أنها تواجه أيضاً تهديدات متعلقة بالفضاء الإلكتروني، تزداد من حيث تعقيدها ودرجة خطورتها، وقد لاحظ الكاتب تغير طبيعة التهديدات الإلكترونية التي تواجهها الولايات المتحدة خلال السنوات العشر الماضية، من اختراق أو إغلاق مواقع إلكترونية، إلى سرقة معلومات عسكرية واقتصادية وتسريب وثائق سياسية وسرقة أنظمة حربية، ويزداد الأمر خطورة مع ربط معظم البنى التحتية الأمريكية، سواء كانت مدنية أو عسكرية بالفضاء الإلكتروني، مثل أنظمة الاتصالات والمواصلات وإدارة المنشآت النووية ومحطات توليد الطاقة الكهربائية ونظم إدارة السدود المائية، إضافة إلى أنظمة توجيه الصواريخ عن بعد والطائرات من دون طيار والسيطرة على الأقمار الصناعية وغيرها، لذا فإن الحفاظ على هذه البنية من أي هجمات إلكترونية يدخل في صميم الأمن القومي الأمريكي، لأن تعرض أحد هذه الأنظمة لهجوم إلكتروني يمكن أن يولد آلاف الضحايا في دقائق معدودة، فمثلاً اختراق نظام المواصلات كأنظمة ملاحة الطيران والسفن وأنظمة السكك الحديد والعبث بها قد يؤدي إلى تصادمها ويعرض الولايات المتحدة لبيرل هاربر جديد، ومن ثم فإن خلق نظام دفاع إلكتروني فعال يعمل بمنزلة حائط صد للهجمات الإلكترونية أمر حيوي للأمن القومي الأمريكي.

وفيما يتعلق بأهم التهديدات الإلكترونية التي تواجه الولايات المتحدة يمكن تحديدها في التالي:

- الإرهاب الإلكتروني.
- استهداف البنى التحتية الحرجة.
- التلاعب بالبيانات العسكرية والاقتصادية.
- تسريب البيانات والمعلومات السرية.
- سرقة حقوق الملكية الفكرية وبراءات الاختراع.

- التحويل غير الشرعي للأموال عبر الإنترنت.
- العنصر البشري الموثوق به.

وحول التساؤل الخاص بالقوة الإلكترونية في العقيدة الأمريكية خلال فترة الدراسة فنجد أنها احتلت مكانة مهمة، سواء في فكر إدارة الرئيس بوش أو فكر إدارة الرئيس أوباما، مع اختلاف كلا الإدارتين في النظر إلى الفضاء الإلكتروني، فبينما نظرت الأولى له على أنه مصدر لتهديد الأمن القومي الأمريكي، وأعدت استراتيجيتها انطلاقاً من هذه الرؤية لتقوم على تعظيم عملياتها العسكرية في الفضاء الإلكتروني، فإن إدارة الرئيس أوباما نظرت إلى الفضاء الإلكتروني باعتباره أحد مصادر رخاء الدولة، وانطلقت استراتيجياتها من العمل على الشراكة مع القطاع الخاص لتأمين وتطوير الفضاء الإلكتروني، ودعت إلى تعاون دولي مشترك لخلق بيئة إلكترونية آمنة، وفي كلا الإدارتين كان البعد الأمني هو الغالب على استراتيجيات الفضاء الإلكتروني، سواء من خلال تطوير قدرات هجومية أو دفاعية.

- وقد نجحت الولايات المتحدة الأمريكية إلى حد كبير في توظيف القوة الإلكترونية لخدمة أهدافها السياسية والعسكرية، فقد كشفت تسريبات سنودن عن البعد الجديد في عمليات التجسس الأمريكي، سواء من خلال التجسس على عدد كبير من الأفراد حول العالم، أو التجسس على الشخصيات الرسمية ورؤساء الدول، أو التجسس على المواطنين الأمريكان أنفسهم، بالإضافة إلى تطوير وكالة الأمن القومي الأمريكي العديد من البرامج التي تسمح بالمراقبة والتجسس والتتبع وصد الهجمات المضادة، وابتكار أدوات تسمح للولايات المتحدة بالتنبؤ بالهجمات الإلكترونية، وكذلك تطوير أدوات تسمح بسرقة المعلومات الاستراتيجية من أجهزة الكمبيوتر غير المتصلة بالإنترنت مما يعد نقلة نوعية في عالم التجسس، وقدرتها على الانتقال ببرمجة الفيروسات من مرحلة التعامل مع البيانات إلى مرحلة التعامل مع المكونات المادية نفسها كما اتضح في فيروس ستاكسنت.

- وعلى الرغم من ذلك التطور، فإن الولايات المتحدة قد وقعت ضحية أيضاً لهجمات إلكترونية سواء من الصين أو روسيا أو إيران، واستطاعت هذه

الهجمات نقل معلومات استراتيجية حول صناعات عسكرية أمريكية ومعلومات تجارية واقتصادية خاصة بالبنوك والشركات والصناعات الحيوية في الولايات المتحدة، مما يمكن اعتباره خصماً من التقدم والرفاهية الأمريكية لصالح هذه الدول.

ومن خلال متابعة نمط إدارة الولايات المتحدة لتفاعلاتها الدولية خلال فترة الدراسة، نجد أنها تميزت بالتالي:

الواقعية في إدارة التفاعلات الدولية:

من خلال متابعة التفاعلات الأمريكية الدولية يتضح أنها تنتهج من المدرسة الواقعية مدخلاً لممارسة علاقتها الدولية، والتي ترتكز على القوة كأساس لإدارة التفاعلات الدولية، في ظل نظام عالمي يتسم بالفوضوية، فالولايات المتحدة تسعى لتعظيم قوتها من خلال إضافة بعد جديد لها وهو القوة الإلكترونية، يضاف إلى جانب القوة الصلبة والقوة الناعمة والقوة الذكية، وتقوم بممارسة هذا النوع من القوة في ظل فضاء إلكتروني يتسم بالفوضوية، ويقصد بالفوضوية هنا عدم وجود سلطة أو حكومة عالمية تقوم بتنظيم مدخلاته ومخرجاته، التي تشترك فيها جميع الفواعل سواء كانت دولية أو من غير الدول، دون الاعتراف بجنس أو جنسية أو عمر أو أيديولوجية.

وعلى الرغم مما هو سائد بأن الأفراد والشركات لهم اليد العليا إدارة الفضاء الإلكتروني، يرى الكاتب أن الولايات المتحدة لم تترك لهم هذه المهمة، حيث عملت الحكومات الأمريكية المتعاقبة خلال فترة الدراسة على إنشاء استراتيجيات تحكم التفاعلات المدنية والعسكرية في هذا الفضاء، وعلى الرغم من ريادة القطاع الخاص في تحقيق التقدم التكنولوجي في هذا المجال، فإن وكالة الأمن القومي الأمريكي عملت على استحداث أنظمة وبرامج تكنولوجية أكثر تقدماً للمراقبة والتجسس، ليس على الحكومات المعادية أو الصديقة فحسب، بل على المواطنين الأمريكيين أيضاً، وهو ما ظهر في الوثائق التي تم تسريبها.

الاعتماد المتزايد على القوة الإلكترونية في إدارة التفاعلات الدولية:

فقد عمدت الإدارات المتعاقبة على البيت الأبيض، سواء خلال فترتي بوش أو أوباما على إنشاء العديد من الخطط والاستراتيجيات التي تتنوع ما بين **الهجوم**، مثل الاستراتيجية القومية العسكرية لعمليات الفضاء الإلكترونية الصادة في 2006، وإنشاء قيادة عسكرية في الفضاء الإلكتروني تابعة لوزارة الدفاع "البنتاجون" الصادرة في 2009، **والدفاع**، مثل الاستراتيجية القومية للحماية المادية للبنية التحتية الحرجة والأصول الرئيسية والاستراتيجية القومية لتأمين الفضاء الإلكتروني الصادرتين في 2003، **وتعظيم التعاون الدولي** في مجال مكافحة الهجمات الإلكترونية، مثل الاستراتيجية الدولية للفضاء الإلكتروني الصادرة في 2011.

وقد تم النظر إلى الفضاء الإلكتروني في الاستراتيجية القومية العسكرية لعمليات الفضاء الإلكترونية The National Military Strategy For Cyberspace Operations على أنه "مسرح لعمليات عسكرية ممكنة"، كما تنظر استراتيجية الأمن القومي الأمريكي عام 2010 إلى أن التهديدات الإلكترونية تمثل واحدة من أخطر التهديدات التي تواجه الأمن القومي والسلامة العامة للمواطنين، فضلاً عن أنها من أهم التحديات التي تواجه الاقتصاد القومي، ومن ثم يجب تأمينها وأن تكون جديرة بثقة مستخدميها، ويمكن تحقيق ذلك عبر الاستثمار في الناس والتكنولوجيا، وتدعيم الشركات مع القطاعات المختلفة، سواء أفراداً أو مؤسسات خاصة. بالإضافة إلى ذلك تقوم وزارة الدفاع الأمريكية بصفة دورية بإجراء محاكاة للتعرض لحرب إلكترونية فيما يطلق عليه Cyber Storm أو عاصفة الحواسب، كما عملت على تطوير أسلحة إلكترونية تشمل فيروسات قادرة على تخريب شبكات العدو.

على الرغم من أن الولايات المتحدة أكثر الدول تقدماً في مجال الهجمات الإلكترونية، فإنها مازالت تحتاج لزيادة قدراتها الدفاعية، فالحرب ليست هجوماً فقط، بل هجوم ودفاع، وهذا لأن جميع القطاعات الحيوية والبنى التحتية الحرجة

في الولايات المتحدة تعتمد بصورة مباشرة على الفضاء الإلكتروني، مما يجعل منها أهدافاً متعددة يمكن إصابتها وتتسبب في شل حركة الدولة الأمريكية.

كما أن الأمر لا يقتصر على تأمين شبكات البنتاجون السرية وغير السرية، بل يشمل أيضاً تأمين شبكات المقاولين العسكريين وشركات صناعة الأسلحة التي تعتمد هي الأخرى على الفضاء الإلكتروني، مما يجعلها عرضة للتهديدات الإلكترونية، ولتأمين البنية التحتية الأمريكية، خاصة المدنية، فإن الأمر يحتاج إلى مليارات الدولارات، خاصة أن الشركات الخاصة هي التي تسيطر على البنية التحتية وتديرها، كما أنها لن تقوم بدفع مليارات الدولارات من أجل زيادة وسائل التأمين لهذه البنية، إلا بتدخل ودعم حكومي مباشر.

الحاجة إلى استراتيجية جديدة لإدارة التفاعلات الدولية في ظل انعدام الخصوصية:

إن كانت الولايات المتحدة قد وضعت من الخطط والاستراتيجيات بعد نهاية الحرب العالمية الثانية، ما يمكنها من إدارة علاقاتها الدولية، وتحقيق أهدافها الاستراتيجية، في فترة تم تشبيهها بالحرب الباردة، فإن الظروف الدولية في أوائل الألفية الثانية أكثر تعقيداً من الخمسين عاماً التي تسبقها، فإذا كانت القوة العسكرية هي المحرك الرئيسي للعلاقات الدولية، فإن هذا المفهوم قد تغير ولم تعد الاستراتيجيات الخاصة بالحروب التقليدية أو حتى غير التقليدية كاستخدام الأسلحة النووية تجدى كثيراً في تحقيق أهداف السياسة الخارجية للدول، فالتغيرات التي طرأت على مفهوم القوة وتحولاتها وتطبيقاتها، غيرت من موازين القوى العالمية، فأصبح امتلاك التكنولوجيا الحديثة وتوظيفها في كافة المجالات السياسية والعسكرية والاقتصادية، أحد أهم أدوات إدارة العلاقات الدولية، وإذا كان العدو في الحرب الباردة معروفاً وواضحاً، ويمكن تعقبه والتنبؤ بسلوكه، فإن الأمر مختلف تماماً في حالة الحرب الإلكترونية، فالعدو ليس بالضرورة دولة، وليس بالضرورة له

جوار جغرافي، بل قد يكون داخلياً، كما أن استهداف المناطق والخدمات الاستراتيجية، أصبح أقل تكلفة من الحرب التقليدية، بل وأكثر تدميراً في بعض الأحيان إذا كان الأمر يتعلق بالسيطرة على البنى التحتية والخدمات اللوجستية سواء مدنية كانت أو عسكرية.

تعرضت الولايات المتحدة خلال فترة الدراسة لبعض المشاكل الدبلوماسية، وإن دق الوصف فهو بمنزلة إحراج دبلوماسي، وذلك من خلال تسريب العديد من الوثائق، سواء التي قام بها أسانج أو سنودن، أظهرت لحلفاء الولايات المتحدة الطريقة التي تتعامل بها معهم، الأمر الذي وصل لحد التجسس على هاتف المستشارة الألمانية أنجيلا ميركل، حيث تزامنت هذه الترسيبات مع مشكلات آنية، ووضعت الولايات المتحدة في حرج أمام حلفائها، جعلت الويات المتحدة تبحث عن تبريرات لتصرفاتها، وعادة ما كان التبرير الأساسي هو العمل لصد الهجمات الإرهابية قبل وقوعها، وهو مبرر غير مقبول، خاصة إذا كان رؤساء الدول أيضاً موقع رصد ومراقبة، وهو ما يعكس دور المخابرات الأمريكية في ممارسة القوة الإلكترونية لتحقيق أهداف الولايات المتحدة الخارجية، من خلال مراقبة رؤساء الدول والحكومات والوزراء ليس لتحقيق أمنية فحسب، بل وأيضاً لتحقيق أهداف سياسية واقتصادية.

وقد فتحت هذه التسريبات الباب أمام الحاجة إلى إعادة النظر في إدارة العلاقات الدولية، فلم تعد تتسم بالسرية أو الخصوصية، فالمحادثات يمكن مراقبتها، والوثائق يمكن تسريبها، والاستراتيجيات التفاوضية والعسكرية يمكن سرقتها، فالاستراتيجيات والتكتيكات التقليدية لإدارة العلاقات الدولية لم تعد مجدية، بل يجب أن تواكب عصر التقدم التكنولوجي، وتعتمد الاستراتيجيات الجديدة على المكاشفة، والاستعداد في أي وقت لمواجهة الرأي العام الدولي والمحلي بالمبررات التي دفعت لاتخاذ مثل هذه القرارات، حتى لا تفقد الحكومة مصداقيتها داخلياً وخارجياً.

النتائج

سعت هذه الدراسة لمعرفة أبرز التطورات التي طرأت على مفهوم القوة وتحولاتها، وإلقاء مزيد من الضوء على مفهوم القوة الإلكترونية، بالإضافة إلى معرفة أثر التكنولوجيا الحديثة وبخاصة الفضاء الإلكتروني على مفهوم انتشار القوة وكذلك تأثيراته على الأمن القومي للدول وبخاصة الولايات المتحدة الأمريكية، وفي هذا الإطار تم الوقوف على عناصر القوة الإلكترونية وأبعاد استخدامها في التفاعلات الدولية سواء كانت سياسية أو اقتصادية أو عسكرية، وتحديد مصالح الولايات المتحدة الأمريكية في الفضاء الإلكترونية ومصادر التهديد التي يمكن أن تواجهه، ومعرفة عناصر القوة الإلكترونية الأمريكية من حيث الاستراتيجيات والأدوات والبرامج خلال الفترة من 2001 حتى 2012، كما وضحت الرسالة أبرز الحدود المفروضة على ممارسة القوة الإلكترونية الأمريكية سواء كانت حدود فنية أو مؤسسية أو قانونية أو السياسية.

وقد توصلت الرسالة إلى عدة نتائج أهمها:

- **الواقعية في إدارة التفاعلات الدولية:** حيث تنتهج الولايات المتحدة الأمريكية من المدرسة الواقعية مدخلاً لممارسة علاقتها الدولية، والتي ترتكز على القوة كأساس لإدارة التفاعلات الدولية، في ظل نظام عالمي يتسم بالفوضوية، وهي في هذا الصدد تسعى لتعظيم قوتها الإلكترونية، في ظل فضاء إلكتروني يتسم بالفوضوية.

- **الاعتماد المتزايد على القوة الإلكترونية في إدارة التفاعلات الدولية:** فقد عمدت الإدارات المتعاقبة سواء خلال فترتي بوش أو فترة أوباما على إنشاء العديد من الخطط والاستراتيجيات التي تتنوع ما بين الهجوم والدفاع وتعظيم التعاون الدولي في مجال مكافحة الهجمات الإلكترونية.

- الحاجة إلى استراتيجية جديدة لإدارة التفاعلات الدولية في ظل انعدام الخصوصية: حيث تعرضت الولايات المتحدة نتيجة استخدامها المتزايد للقوة الإلكترونية لبعض المشاكل الدبلوماسية، وإن دق الوصف فهي بمثابة إحراج دبلوماسي، وذلك من خلال تسريب العديد من الوثائق سواء التي قام بها ويليام أسانج أو أدوردسنودن وقد فتحت هذه التسريبات الباب أمام الحاجة إلى إعادة النظر في إدارة العلاقات الدولية، فلم تعد تتسم بالسرية أو الخصوصية.

المصادر والمراجع

أولاً: المراجع باللغة العربية:

الكتب:

1- أحمد يوسف أحمد، د. محمد زبارة، **مقدمة في العلاقات الدولية**، القاهرة: مكتبة الأنجلو المصرية، 1985.

2- إسماعيل صبري مقلد، **العلاقات السياسية الدولية: النظرية والواقع**، كلية التجارة: جامعة أسيوط، الطبعة الرابعة، 2004.

3- ايثيلدوسولابول، **التكنولوجيا والسياسة في عصر المعلومات**، ترجمة ماري عوض، تونس: المنظمة العربية للتربية والثقافة والعلوم، 1980.

4- حسن طاهر داود، **جرائم نظم المعلومات**، الرياض: أكاديمية نايف العربية للعلوم الأمنية، 2000.

5- ريتشارد كلارك وروبرت نيك، **حرب الفضاء الإلكتروني** .. التهديد التالي للأمن القومي وكيفية التعامل معه، أبوظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية، الطبعة الأولى، 2012.

6- عادل عبدالصادق، **الإرهاب الإلكتروني، القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة**، القاهرة: مركز الأهرام للدراسات السياسية والاستراتيجية، 2009.

7- عباس بدران، **الحرب الإلكترونية .. الاشتباك في عالم المعلومات**، لبنان: مركز دراسات الحكومة الإلكترونية، 2010.

8- عبدالعزيز العيادي، **ميشيل فوكو.. المعرفة والسلطة**، المؤسسة الجامعية للدراسات والنشر والتوزيع، الطبعة الأولى، 1994.

9- الفن توفلر، **تحول السلطة**، ترجمة لبنى الريدي، القاهرة: الهيئة المصرية العامة للكتاب، 1995.

10- منير محمد الجنبيهي، **أمن المعلومات الإلكترونية**، القاهرة: دار الفكر الجامعي، 2005.

الدوريات:

1- إيمان رجب (محررة)، "القوة: كيف يمكن فهم تحولات القوة في السياسة الدولية"، **ملحق اتجاهات نظرية في تحليل السياسة الدولية،مجلة السياسة الدولية**، العدد رقم 188، أبريل 2012.

2- باهر عصمت، الإنترنت ومنظمة الآيكان، **مجلة السياسة الدولية**، العدد رقم 180، أبريل 2010.

3- جمال محمد غيطاس، "إدارة الإنترنت وإرهاصات التحول من الهيمنة إلى التعددية"، **مجلة السياسة الدولية**، عدد رقم 180، أبريل 2010.

4- حسن أبو طالب، الفجوة الرقمية والتنمية في ظل العولمة، **مجلة السياسة الدولية**، عدد رقم 180، أبريل 2010.

5- ريهام مقبل، "مركب القوة: عناصر وأشكال القوة في العلاقات الدولية"، في إيمان رجب (محرر)، **ملحق اتجاهات نظرية في تحليل السياسة الدولية، مجلة السياسة الدولية**، ملحق اتجاهات نظرية، عدد رقم 188، أبريل 2012.

6- سعاد محمود أبو ليلة، "دورة القوة: ديناميكيات الانتقال من "الصلبة" إلى "الناعمة" إلى "الافتراضية"، **مجلة السياسة الدولية**، ملحق اتجاهات نظرية، عدد رقم 188، أبريل 2012.

7- عادل عبدالصادق، "الفضاء الإلكتروني وتهديدات جديدة للأمن القومي"، **مجلة السياسة الدولية**، عدد رقم 180، أبريل 2010.

8- عادل عبدالصادق، القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، **مجلة السياسة الدولية**، عدد رقم 188، أبريل 2012.

9- عادل عبدالصادق، "مصر ومجتمع المعلومات: هل يمكن تكرار التجربة الهندية؟"، **مجلة تعليقات مصرية**، العدد 17، يوليو 2004.

10- علي جلال معوض، "إعادة الانتشار: تحليل أولي لأبعاد وآثار انتشار القوة داخل وبين الدول"، في إيمان رجب (محرر)، **ملحق اتجاهات نظرية في تحليل السياسة الدولية، مجلة السياسة الدولية**، عدد رقم 188، أبريل، 2012.

11- محمد أبورمان، "تنظيم القاعدة والإنترنت .. تدشين الجيل الثالث من الجهاديين"، **مجلة السياسة الدولية**، عدد رقم 180، أبريل 2010.

12- محمد عبدالسلام، "استخدامات القوة: كيف يمكن التأثير في سلوك الفاعلين الدوليين"، في إيمان رجب (محرر)، **ملحق اتجاهات نظرية في تحليل السياسة الدولية، مجلة السياسة الدولية**، ملحق اتجاهات نظرية، عدد رقم 180، أبريل 2010.

13- معتز سلامة، "استراتيجية الأمن القومي الأمريكي 2010"، **كراسات استراتيجية**، عدد 165، أبريل 2010.

14- ميلاد بورنيك، "الإنترنت والمعارضة السياسية .. الحالة الإيرانية"، **مجلة السياسة الدولية**، عدد رقم 180، أبريل 2010.

15- وليد رشاد زكي،الشبكات الاجتماعية .. محاولة للفهم، **مجلة السياسة الدولية**، عدد رقم 180، أبريل 2010.

الدراسات والمقالات:

1- أدهم عدنان طبيل، **الإعلام الحديث في ظل العولمة**، صحيفة دنيا الوطن الإلكترونية، 25 مايو 2007، يمكن المطالعة على:

http://pulpit.alwatanvoice.com/articles/2007/05/25/89911.html

2- إسراء أحمد وشريف رشدي، **"الواقع الافتراضي والتغيير السياسي في العالم، دراسة في ثورات الوطن العربي"**، مركز المعلومات ودعم اتخاذ القرار، يونيو 2011.

3- أولاف تايلر، **التهديدات الجديدة: الأبعاد الإلكترونية**، مجلة حلف الناتو، 11 سبتمبر 2011، يمكن المطالعة على الرابط التالي:

http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/AR/index.htm

4- إيريك شميت وتوم شانكر، **واشنطن تكافح الإرهاب العالمي بأسلوب الحرب الباردة**، موقع الشرق الأوسط، تاريخ دخول 20 مارس 2008، يمكن المطالعة على:

:http://classic.aawsat.com/details.asp?section=4&article=463429&issueno=10705#.VG9PVvmsU00

5- إيهاب عبدالحميد خليفة، **الفضاء الإلكتروني وتهديدات الأمن القومي المصري**، المركز العربي لأبحاث الفضاء الإلكتروني، بتاريخ 22 أغسطس 2013، يمكن المطالعة على:

http://www.accronline.com/print_article.aspx?id=15383

6- إيهاب عبدالحميد خليفة، **القوة الإلكترونية والصراع الدولي**، مقال منشور على موقع المركز العربي لأبحاث الفضاء الإلكتروني، 30 أغسطس 2013، يمكن المطالعة على:

http://www.accronline.com/print_article.aspx?id=15636

7- باربرا سلافين، وجيسون هيلي، الحرب الافتراضية: هل تملك طهران القدرة على مهاجمة واشنطن إلكترونياً؟، المركز الإقليمي للدراسات السياسية والاستراتيجية، 14 أبريل 2014.

8- د. أولاف تايلر، **التهديدات الجديدة: الأبعاد الإلكترونية**، مجلة الناتو، بتاريخ مطالعة 23 مارس 2013، يمكن المطالعة على:

http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/AR/index.htm

9- رفيق عبدالسلام، **الولايات المتحدة الأمريكية بين القوة الصلبة والقوة الناعمة**، مركز الجزيرة للدراسات، 2008.

10- شيريهان نشأت المنيري، **الإرهاب الإلكتروني**، موقع السياسة الدولية، 12 نوفمبر 2013.

11- عادل عبدالصادق، "الصين وجوجل .. أزمة متعددة الأبعاد"، موقع **بوابة الأهرام**، بتاريخ دخول 18 أبريل 2014، يمكن المطالعة على:

http://www.ahram.org.eg/archive/The-Writers/News/16447.aspx

12- كريم خشبة، **تسريبات سنودن: إدارة العلاقات الدولية في عصر التسريبات**، تحليل منشور على موقع المركز الإقليمي للدراسات الاستراتيجية، بتاريخ مطالعة 1 يوليو 2014، يمكن المطالعة على:

http://goo.gl/CNLVws

13- لوران جيسيل، **قانون الحرب يضع قيوداً على الهجمات الإلكترونية أيضاً**، مقال منشور على موقع اللجنة الدولية للصليب الأحمر، بتاريخ 1يوليو 2013، للمطالعة:

http://www.icrc.org/ara/resources/documents/interview/2013/06-27-cyber-warfare-ihl.htm

14- مجلة حلف الناتو، **تاريخ الهجمات الإلكترونية**، 18 أبريل 2014.

15- محمد الحسين، **الحرب الافتراضية: هل تملك طهران القدرة على مهاجمة واشنطن إلكترونياً**؟ المركز الإقليمي للدراسات الاستراتيجية، بتاريخ مطالعة 10 سبتمبر 2013، يمكن المطالعة على الرابط التالي:

http://goo.gl/ybPy92

16- مركز الصحوة للدراسات، **القوة الناعمة الأمريكية آفاقها وتحدياتها**، 13 نوفمبر 2012.

17- نسرين فوز اللواتي، **سباق التسلح التكنولوجي بين أمريكا والصين**، مجلة لغة العصر، نوفمبر 2013.

18- نوران شفيق علي، الثقة المفقودة: تداعيات أزمة التجسس الأمريكي على الدول الأوروبية، **الموقع الإلكتروني لمجلة السياسة الدولية**، تاريخ دخول 3 نوفمبر 2013.

19- هبة رؤوف عزت، **القوة الناعمة المهدرة: أزمة النظام القوي والدولة الضعيفة بمصر**، مركز الجزيرة للدراسات، أكتوبر 2011.

مصادر أخرى:

1- إدارة أوباما تقر بأن وكالة الأمن القومي انتهكت قانون مراقبة الاتصالات، موقع إيلاف، بتاريخ 6 سبتمبر 2013، يمكن المطالعةعلى:

http://www.elaph.com/Web/news/2013/8/831530.html#sthash.JweuZei0.dpuf

2- أزمة الميزانية الأمريكية: إغلاق دوائر حكومية فيدرالية بسبب الخلاف، موقع BBC، بتاريخ 17 نوفمبر 2013.

http://www.bbc.co.uk/arabic/worldnews/2013/10/131001_us_budget_shutdown.shtml

3- الحرب الإلكترونية، موقع اللجنة الدولية الصليب الأحمر، 29 أغسطس 2014.

4- الجيل الجديد من المحاربين الكمبيوتريين في الولايات المتحدة وإسرائيل، مجلة الكمبيوتر والاتصالات والإلكترونيات، العدد 9، المجلد 30، نوفمبر 2013.

5- الاستخبارات الأمريكية تجسست على إسلاميين متشددين يدخلون مواقع إباحية، موقع فرنسا 24، بتاريخ 28نوفمبر2013، يمكن المطالعة على:

http://goo.gl/nUiF21

6- الاستخبارات الأميركية تخشى وجود إدوارد سنودن آخر في صفوفها، موقع جريدة الحياة، بتاريخ 6 أغسطس 2014، يمكن المطالعة على:

http://goo.gl/0JKAkH

7- استراتيجية البنتاغون لأمنها الإلكتروني، تقرير منشور على موقع الجزيرة، بتاريخ 15 يوليو 2011، يمكن المطالعة على:

http://goo.gl/TT18B3

8- أمريكا تتهم الصين بسرقة تكنولوجيا صنع مقاتلة "أف – 35"، موقع روسيا اليوم، بتاريخ 14 مارس 2014، يمكن المطالعة على:

http://arabic.rt.com/news/668023

9- انونيموس .. القراصنة المجهولون، موقع الجزيرة، بتاريخ 5فبراير 2013، مطالعة على:

http://www.aljazeera.net/news/pages/063cb2e9-5134-4509-a278-6eab43f8bd65?GoogleStatID=9

10- اتفاق تاريخي يمنح منظمة الآيكان استقلالية كبرى عن الحكومة الأمريكية، بوابة الأهرام، بتاريخ 13أكتوبر 2009، يمكن المطالعة على:

http://digital.ahram.org.eg/articles.aspx?Serial=6937&eid=1297

11- أوباما أمر بوقف تجسس وكالة الأمن القومي على مقري صندوق النقد الدولي والبنك الدولي، وكالة رويترز، بتاريخ1نوفمبر 2013، يمكن المطالعة على:

http://ara.reuters.com/article/worldNews/idARACAE9B2C3S20131101

12- أوباما لم يكن على علم بـ"التجسس على هاتف ميركل"، موقع BBC، بتاريخ 19 أبريل 2014، يمكن المطالعة على:

http://www.bbc.co.uk/arabic/worldnews/2013/10/131027_obama_merkel_phone_spy_row.shtml

13- إيران تسقط طائرة استطلاع أمريكية بدون طيار، وكالة رويترز للأنباء، تاريخ 17 ديسمبر 2011، على الرابط التالي:

http://arabic.rt.com/news/573311/

14- إيران تؤكد اختراق أسرار الطائرة الأميركية آر كيو-170، موقع إيلاف الإخباري، بتاريخ 24 أبريل 2012، يمكن المطالعة على:

http://www.elaph.com/Web/news/2012/4/731015.html#sthash.eQfwfoLU.dpuf

15- الآيكان" تعطي الضوء الأخضر لتدوين عناوين مواقع الإنترنت باللغة العربية، خبر منشور على موقع فرانس 24، بتاريخ 6 يونيو 2010، يمكن المطالعة على الرابط التالي:

http://www.france24.com/ar/20100506-multimedia-internet-icann-organisation-arabic-url-authorization-alphabetic-letter

16- برلين تستدعي السفير الأميركي حول التجسس على ميركل، العربية نت،24أكتوبر 2013، يمكن المطالعة

http://goo.gl/x8W5gd:

17- تأجيل معركة رفع سقف الدَّين وإغلاق الحكومة الأمريكية، موقع جريدة الاقتصادية، بتاريخ 18أكتوبر 2013،

http://www.aleqt.com/2013/10/18/article_793563.html

18- تايلاند تقبض على "قرصان البنوك" الجزائري حمزة بن دلاج، خبر منشور على موقع BBC، بتاريخ 8 يناير 2013، تاريخ دخول 8 أغسطس 2014، يمكن المطالعة على:

http://www.bbc.co.uk/arabic/worldnews/2013/01/130108_thailand_algeria_usa_bank_hacking.shtml

19- تسريبات لسنودن تكشف تجسس أمريكا وبريطانيا على أولمرت ومسؤول أوروبي، وكالة رويترز للأنباء بتاريخ 20 ديسمبر 2013، يمكن المطالعة على

:http://ara.reuters.com/article/worldNews/idARACAE9BJ0C820131220?pageNumber=2&virtualBrandChannel=0

20- تقرير: الولايات المتحدة تجسست على هاتف ميركل منذ 2002، خبر منشور على موقع BBC، بتاريخ دخول 26أكتوبر 2013، يمكن المطالعة على

http://www.bbc.co.uk/arabic/worldnews/2013/10/131026_us_bugged_merkel.shtml

21- جرائم الإنترنت كلفت الصين أكثر من 46 مليار دولار، المركز العربي لأبحاث الفضاء الإلكتروني، 20 أغسطس 2013.

22- جوجل.. حصان طروادة في الصين، موقع بوابة الأهرام، تاريخ العدد 28 يناير 2010، يمكن المطالعة على:

http://digital.ahram.org.eg/articles.aspx?Serial=197049&eid=1769

23- الحرب الإلكترونية أخطر تهديد إيراني، تقرير منشور على موقع CNN، بتاريخ 7 نوفمبر 2013، يمكن المطالعة على:

http://archive.arabic.cnn.com/2012/scitech/11/6/_iran-cyberattack/

24- الحكم بالسجن 35 عاماً على الجندي الأمريكي برادلي مانينغ في قضية "ويكيليس"، موقع France 24 بتاريخ 21 أغسطس 2013،

http://goo.gl/QI0TUn

25- خبراء: الحرب الإلكترونية أخطر تهديد إيراني، موقع CNN، 7 نوفمبر2012، يمكن المطالعة على:

http://arabic.cnn.com/2012/scitech/11/6/_iran-cyberattack/index.html

26- رعب في أمريكا من الحرب الإلكترونية، موقع بوابة الأهرام، بتاريخ نشر ومطالعة 21 أكتوبر 2013، يمكن المطالعة على:

http://www.ahram.org.eg/The-First/News/178157.aspx

27- الصين تحجب خدمات «جوجل» عن مواطنيها، جريدة الاقتصادية، بتاريخ 11 نوفمبر، 2012

http://www.aleqt.com/2012/11/11/article_708496.html

28- فرنسا تستدعي السفير الأمريكي في باريس لمناقشة تهم بالتجسس على ملايين الفرنسيين، خبر منشور على موقع BBC بتاريخ 13 أكتوبر 2013، يمكن المطالعة على:

http://www.bbc.co.uk/arabic/worldnews/2013/10/131021_france_us_spying_crisis.shtml

29- قراصنة كمبيوتر يسرقون معلومات شخصية من شركة أمنية أمريكية، خبر منشور على موقع BBC بتاريخ 11 ديسمبر 2013

http://www.bbc.co.uk/arabic/scienceandtech/2011/12/111225_hackers_us_security.shtml

30- محاكمة جنائية لأكبر شبكة غسيل أموال في مصر وأمريكا، خبر منشور بموقع الأهرام الرقمي، بتاريخ 9 فبراير 2010، يمكن المطالعة على:

http://digital.ahram.org.eg/articles.aspx?Serial=57999&eid=1387

31- هاكر جزائري يكشف تفاصيل الحرب الإلكترونية على إسرائيل، خبر منشور على موقع العربية نت، بتاريخ 10 أبريل 2013،

http://goo.gl/3crCLx

32- هجوم إلكتروني يهدد بتدمير أمريكا في 15 دقيقة، خبر منشور هسبرس ، بتاريخ 9 مايو 2010، يمكن المطالعة على:

http://www.hespress.com/international/20914.html

33- هل يستمر احتكار الولايات المتحدة لإدارة الإنترنت؟، تقرير منشور على موقع BBC، بتاريخ مطالعة 15نوفمبر 2005، يمكن المطالعة على الرابط التالي

http://news.bbc.co.uk/hi/arabic/sci_tech/newsid_4440000/4440840.stm

34- واشنطن تطلق سفارة افتراضية لدى طهران على الإنترنت، خبر منشور على موقع اليوم السابع، بتاريخ مطالعة 26ديسمبر 2011، للمزيد يمكن المطالعة على

http://www1.youm7.com/News.asp?NewsID=548853&SecID=286&IssueID=0#.U1wTP4GSwoI

35- واشنطن تندد بحجب طهران " سفارتها الافتراضية" على الإنترنت، خبر منشور على موقع BBC بتاريخ دخول 5 ديسمبر 2011، يمكن المطالعة على:

http://www.bbc.co.uk/arabic/worldnews/2011/12/111207_iran_us_embassy_virtual_internet.shtm

ثانياً: المراجع باللغة الأجنبية:

Documents:

1- "Cyberspace Policy Review", The Office of the White House, May 29th, 2009.

2- "Deterrence Operations, Joint Operating", Department of Defense, Concept, Washington, DC, December 2006.

3- "Draft Declaration on Rights and Duties of States", 1949, art. 2

4- "Federal Information Security Management Act (Fisma) Implementation Project", National Institute of Standards and Technology, August 30th, 2014

5- "International StrategyFor Cyberspace", The White House, May 2011.

6- "National Strategy to Secure Cyberspace", Hathaway, Melissa, Washington DC: The White House, May 2009.

7- "Occupational Employment Statistics", Bureau of Labor Statistics, occupational employment and wage estimates, nationalcross-industry estimates, May 2001, May 2011; accessed July 17th, 2014.

8- Rogin, Josh, "Cartwright: Cyber Warfare Strategy 'Dysfunctional'", U.S. Air Force Aim Points, February 12th, 2007.

9- Schimitt, Michael N., Editor, "Talinn Manual on the international law applicable to cyber warfare", Prepared by the international group of experts at the initiative of NATO cooperative cyber defense of excellence, Cambridge University Press, 2013.

10- "Science and Engineering Indicators 2012", National Science Board , 2012

11- "The Comprehensive National Cybersecurity Initiative ",The White House, 2008

12- "The Implementation of Network-Centric Warfare", Office of Force Transformation, Washington, DC: U.S. Government Printing Office, January 2005.

13- "The National Defense Strategy 2008", Department of defense, Washington DC: Department, June 2008.

14- "The National Defense Strategy of the United States of America", Washington, DC: The Pentagon, March 2005.

15- "The National Military Strategy For Cyberspace Operations", The White House, December 2006.

16- "The National Military Strategyof theUnited Statesof America", The White House, 2004.

17- "The National Military Strategy to Secure Cyberspace (classified)", Department of Defense in early, 2007.

18- "The National Security Strategy of the United States of America", The White House, Washington, DC:March 2006.

19- "The National Security Strategy of the United States of America", The White House, Washington, DC September 2002.

20- "The National Strategy for Homeland Security", The White House, Washington, DC: The White House, February 2003.

21- "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets", The White House, February 2003.

22- "The National Strategy to Secure Cyberspace", The White House, Washington, DC, February 2002.

23- "The Protect America Act", Department Of Justice, August 2007.

24- "The USA PATRIOT Act",Department of justice, October 2001.

Books:

1- Billo, Charles G., Cyber Warfare An Analysis Of The Means And Motivations Of Selected Nation States , (Dartmouth College, Institute For Security Technology Studies, November 2004)

2- Alan, Campen, .; and Dearth, Douglas H., eds, Cyber war 2.0: Myths, Mysteries and reality. (Fairfax. VA, AFCEA International press 1998)

3- Caton, Jeffrey L., Information As Power And America's National Security, (U.S. ARMY WAR COLLEGE, May 2012)

4- Dougherty, James E.; Pfaltzgraff, Robert L., Contending Theories of International Relations, (Longman, 2001)

5- Geers, Kenneth, Cyber Space and the changing nature of warfare, (U.S. Representative Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia. On August 2008)

6- Grant, Rebecca, Victory in cyber space, (The Air Force Association, October 2007)

7- Gregory J. Rattray , An Environmental Approach to Understanding Cyberpower, Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz Editors, Cyber Power and National Security, (Washington, D.C, Center for Technology and National Security Policy., 2009)

8- ------------, Strategic Warfare in Cyberspace, (Cambridge: MIT Press, 2001)

9- Guzzini, Stefano, "Structural power: the limits of neorealist power analysis", International Organizations, Vol. 47, No. 3, (Cambridge, 1993).

10- Kramer, Franklin D.; Starr, Stuart H.; Wentz,Larry; eds, Cyberpower and National Security, (Washington D.C: National defense University, May 2009)

11- Kuehl, Daniel T., "From Cyber Space to Cyber Power: Defining the problems", in Franklin D. Krammer, Stuart Starr, and Larry K. Wentz. Eds, cyber power and national security, (Washington, D.C: National defense up, 2009)

12- Kuehl and Miller, "Cyberspace and the 'First Battle' in 21st-century War," Eugene Habiger, Cyberwarfare and Cyberterrorism: The Need for a New U.S. Strategic Approach, (Washington DC: Cyber Secure Institute, February 1, 2010)

13- Lachow, Irving, "Cyber Terrorism: Menace or Myth?", in D. Kramer, Stuart H. Starr, Larry Wentz ,eds, Cyberpower and National Security, (Washington D.C: National defense University, May 2009)

14- Martin C, Libicki,., "Military Cyberpower", in Franklin D. Kramer, Stuart H. Starr, Larry Wentz , eds, Cyberpower and National Security, (Washington D.C: National defense University, May 2009)

15- Zoller, Lieutenant, Richard g., Russian Cyberspace Strategy And A Proposed United States Response, (U.S. Army War College, Carlisle Barracks, 2010)

16- Lord , Kristin M.; Travis Sharp, Editors, America's Cyber Future: Security And Prosperity In The Information Age, (Center For A New America Security, June 2011)

17- Lukes, Steven,Power: A radical View, (British sociological association ,1974)

18- Morgenthall, Hans J., politics Among Nations, (New York ,Altred A. Kreptp ,1948)

19- Morris, Peter, Power: A philosophical Analysis, (Manchester, Manchester University Press, 1987)

20- Murphy- Dennis M., ed., Information Operations Primer, (Carlisle, Pennsylvania: U.S. Army War College, 2010)

21- Choucri, Nazli, Cyberpolitics in International Relations, (England, The MIT Press Cambridge, Massachusetts London, 2012).

22- Nye, Joseph S. Jr., Soft Power: The means to success in world politics, (New York: Public Affairs, 2004)

23—, Cyber Power, (Cambridge: Harvard Kennedy School, Belfer center for Science and International affairs, May 2010)

24- ———, Soft Power, Hard Power and Leadership, (Harvard Univeristy, October 2006)

25- ———, The Future of Power, (Harvard University, 10 May 2011)

26- Rosenau, James "Capabilities and control in an interdependent world", International Security, Vol. 1 (Fall 1976).

27- Skoudis, Edward, Evolutionary Trends in Cyberspace, Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz Editors, Cyber Power and National Security, (Center for Technology and National Security Policy, Washington, D.C., 2009.)

28- Smith, Craig A., The World wide web of war, (strategy research project, US, Army War college February 2006)

29- Sobel, Jeffery C., Digination: The Birth of Cyber – Nations, (Maxwell AFB, AL, Air Command and Stuff College, 2005)

30- Spade, Colonel Jayson M., China’s Cyber Power andAmerica’s National Security, Edited By Jeffrey L. Caton (U.S. Army War College, 2001)

31- Sullivan, Michael P., International Theroies and Evedence, New Jersy: Prentice –Hall, Inc., (Englewood Chiffs, 1976)

32- Thomas, Timothy L.,"Nation-state Cyber Strategies: Examples from China and Russia", in Franklin D. Kramer, Stuart H. Starr, Larry Wentz ,eds, Cyberpower and National Security, (Washington D.C: National defense University, May 2009)

33- Vatis, Michael A, Cyber Attacks During The War On Terrorism: A Predictive Analysis, (Institute For Security Technology Studies At Dartmouth College, September 2001)

34- Waltz, Man, Keneeth N., The State & War, Athearetical Analysis (N .Y :Colombia Unversity Press , 1959)

35- Zimet, Elihu and Skoudis, Edward, A Graphical Introduction to the Structural Elements of Cyberspace, Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz Editors, Cyber Power and National Security, (Washington, Center for Technology and National Security Policy, , D.C., 2009)

Periodicals:

1- Keith, AlexanderB., "Building A New Command in Cyberspace", Strategic Studies Quarterly, USA, Summer 2011.

2- Finnemore, Martha,"Legitimacy, hypocrisy, and the social structure of unipolarity: why being a unipole isn't all it's cracked up to be", World politics: Quarterly Journal of International Relations, Vol16.,No1., Jan 2009

3- Chang, Frederick R., "Is Your Computer Secure?"*Science, Vol* 325, July 2009

4- Jsamuels, warren, "The Political –Economic logic of world governance", Review of social economy, Vol.59, No3, 2001

5- Nye, Joseph S., "The Decline of America's Soft Power", Foreign Affairs, May/ Jun e 2004.

6- Paganini, Pierluigi, "Stellar Wind, Prism,EvilOlive,ShellTrumpet, US massive surveillance", Security Affairs, on June 29th, 2014.

7- Cybercrime constitutes the "greatest transfer of wealth in history", Foreign Policy: The Cable, on July 12, 2014

Reports:

1- Allison, Graham T., Simes, Dimitri K., Thomson, James. Editors, America's National Interests, The Commission on America's National Interests, July 2000.

2- Armed Forces Communications and Electronics Association,The Evolution of U.S. Cyberpower,Oct 25, 2013

3- Clay, Wilson, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress." (CRS Reports. 29 January 2008).

Department of Defense, 2006 Quadrennial Defense Review Report, Washington, DC: Department of Defense, February 2006.

4- Economist Intelligence Unit, Cyber Power Index, August 2014.

5- FBI, Economic Espionage: Protecting American’s Trade Secrets, on July 2014

6- Foreign spies stealing US Economic Collection and industrial secrets in cyberspace,Office of the National Counterintelligence Executive, October 2011.

7- Global Energy Cyberattacks:"Night Dragon", McAfee® Foundstone® Professional Services and McAfee Labs™, February, 2011.

8- Grant, Rebecca, victory in cyberspace, An Air Force Association Special Report, October 2007.

9- Home Land Security, ICS-CERTMonitor, Oct, Nov, Dec, 2012, June 23th, 2013.

10- James, Lewis A.,ComputerEspionage,Titan Rain and China, CSIS, On May, 2014.

11- James, Lewis A., Securing Cyberspace for the 44the Presidency: A Report of the CSIS Commission on Cybersecurity for the 44the Presidency, Center for Strategic and International Studies, December 2008.

12- Keeping the Nation’s Industrial Base Safe From Cyber Threats, Cyber Threats to National Security, Carnegie Institution for Science, Washington, D.C, September 2011.

13- Libicki, Martin C., Cyberdeterrence and Cyberwar, Santa Monica: RAND, 2009.

14- Mandiat, Exposing one of china’s cyber espionage unites, APT-1, Feb 2013.

15- Peritz, Aki J. &Sechrist, Michael, Protecting Cyberspace and the US National Interest, Harvard Kennedy school, September 2010.

16- Perry, Nick AndDodd, Paisley, 5 Nation Spy Alliance Too Vital For Leaks To Harm, AP, August 29, 2014.

17- President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection, October 1997.

18- Rollins, John, and Chenning, Anna, Comprehensive national cyber security initiative: legal authorities and policy recommendations national cyberstrategy, Congressional research service, March 2009.

19- Shapiro, Robert J. and AparnaMathur, The Contributions of Information and Communication Technologies To American Growth, Productivity, Jobs and Prosperity, September 2011.

20- Shirley A. Kan, U.S.-China Military Contacts: Issues for Congress, Washington, DC: U.S. Library of Congress, Congressional Research Service, December 2010.

21- Spade Jayson M., China's Cyber Power And America's National Security, Jeffrey L. Caton Editor, U.S. Army War College, May 2012.

22- US Army Training and Doctrine Command, Critical Infrastructure: Threats and Terrorism, August 2006.

23- Vatis, Michael, Cyber Attacks During the War on Terrorism: A Predictive Analysis, Institute For Security Technology StudiesAt Dartmouth College, September 2001.

24- Wortzel, Larry, Defense dossier, American Foreign Policy Council, August 2012.

25- Zia DaniellWigder, Global Online Population Forecast, 2008 To 2013, On September 2013.

Newspaper:

1- Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data, The Guardian, Jan 28th, 2014.

2- Brazil demands explanation from US over NSA spying, The Guardian, On July 8 th,2013

3- Chinese Army Unit Is Seen as Tied to Hacking Against U.S, The New York Times, February 18, 2013.

4- Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies, The Washington Post, On March 27th, 2013.

5- Court gave NSA broad leeway in surveillance, The Washington Post documents show, on June 30, 2014.

6- Edward Snowden says motive behind leaks was to expose 'surveillance state', The Washington Post, on June 10, 2013, On

7- Electricity Grid in U.S. Penetrated By Spies, The wall street Journal, April 8, 2009.

8- Global Strategy Stabilized IBM During Downturn, New York Times, April 20, 2010.

9- Hacking U.S. Secrets, China Pushes for Drones, The New York Times, Sep 21, 2013.

10- How the NSA is still harvesting your online data, The Guardian, June 17, 2014.

11- Brazil demands explanation from US over NSA spying, Thr Guardian, July 8, 2013.

12- Iran says Stuxnet virus infected 16,000 computers, Foxnews, On Feb 18, 2012.

13- Justice Department and NSA memos proposing broader powers for NSA to collect data, The Guardian, June27,2013.

14- Misha Glenny, The cyber arms race is on, Post-gazette,October 23, 2011.

15- N.S.A. Devises Radio Pathway Into Computers, The New York Times, On Jan14th, 2014.

16- Nathan Thornburgh,Inside the Chinese Hack Attack, Time, on July Aug. 25, 2005.

17- North Korean hackers may have stolen US war plans, The Guardian, On December 18, 2009.

18- NSA accused of spying on Brazilian oil company Petrobras,The Guardian, on September 9, 2013.

19- NSA monitored calls of 35 world leaders after US official handed over contacts, The Guardian, On October 25, 2013.

20- NSA Prism program slides, The Guardian, On 1 Nov 2013.

21- The cyber arms race is on, as nations large and small mobilize to protect themselves and their enemies if provoked, Post-gazette, October 23, 2011.

22- Timothy B. Lee, Here's everything we know about PRISM to date, The Washington Post, June 12, 2013.

23- U.S. Plans Cyber Shield for Utilities, Companies, The Wall Street Journal, Oct 12, 2013.

24- U.S. ranks second on Cyber Power Index, Federal news radio, Jan 20, 2012.

Internet:

1- Computer worms, On august 10,

2013http://virusall.com/computer%20worms/worms.php

2- Secret program gives NSA, FBI backdoor access to Apple, Google, Facebook, Microsoft data, On June, 6TH,

2013,http://www.theverge.com/2013/6/6/4403868/nsa-fbi-mine-data-apple-google-facebook-microsoft-others-prism/in/4167369z

3- NSA infected 50,000 computer networks with malicious software, Nuclear Regulatory Commission, Nov, 23th, 2013. on http://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software/

4- NSA offers explanation of Perfect Citizen,on Feb 3ed, 2013 http://news.cnet.com/8301-1009_3-20010155-83.html

5- Secret program gives NSA, FBI backdoor access to Apple, Google, Facebook, Microsoft data , June 6th, 2013, on http://www.theverge.com/2013/6/6/4403868/nsa-fbi-mine-data-apple-google-facebook-microsoft-others-prism

6- Shemayve, Volodymyr N., Cognitive approach to modeling reflexive control in Socio-Economic system, On April 22, 2007 On http://infosec.procon.bg/v22/Shemayev_ReflexiveControl.pdf

7- The Evolution of U.S. Cyberpower, Armed Forces

Communications and Electronics Association.

http://www.afcea.org/committees/cyber/documents/TheEvolutionofUSCyberpower.pdf

8- Trojan horse, On 10 August 12th , 2014

http://searchsecurity.techtarget.com/definition/

9- Volodymyr N. Shemayve, Cognitive approach to modeling reflexive control in Socio-Economic system,

http://infosec.procon.bg/v22/Shemayev_ReflexiveControl.pdf On 10December 2012

10- Weimann, Gabriel, Cyberterrorism: How Real Is the Threat?, United States Institute Of Peace, December 2004. On http://www.usip.org/publications/cyberterrorism-how-real-the-threat

11- What is a computer virus?, http://www.microsoft.com/security/pc-security/virus-whatis.aspx On august 10, 2013

12- Everything you need to know about PRISM,August 25, 2014, on http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet

قائمة المحتويات

إيهاب خليفة

المؤهلات الحاصل عليها:

- بكالوريوس اقتصاد وعلوم سياسيه – جامعه القاهرة 2009.

- ماجيستير – إداره العلاقات الدوليه

- باحث دكتوراه فى مجال إداره المدن الذكيه

الابحاث والمؤلفات:

- كتاب "حروب مواقع التواصل الاجتماعى" 2016.

- العديد من الابحاث العلميه المنشوره باللغه العربيه والانجليزيه فى التدعيات الناجمه تزايد الاعتماد على التقنيات الذكيه فى الحياه البشريه ومصادر تهديد الامن القومى.

الخبرات والاعمال:

- رئيس وحدة التطورات التكنولوجية بمركز المستقبل للأبحاث والدراسات المتقدمة

- باحث سابق بمجلس الوزراء المصري.

- وباحث مشارك بالمركز الإقليمي للدراسات الاستراتيجية بالقاهرة

التواصل:

hobaway@gmail.com